Co-funded by the European Union

FinPower

Modul: ONLINE SICHERHEIT UND SCHUTZ

Vorbereitet von: RightChallenge

PROJECT ID NUMBER: 2022-1-AT01-KA220-ADU-000087985

Table of Contents

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

LERNZIELE

Die Lernziele dieses Moduls sind vielfältig und darauf ausgelegt, den TeilnehmerInnen umfassendes Wissen und praktische Fähigkeiten in spezifischen Bereichen zu vermitteln.

Das erste Thema ist „Online-Sicherheit“. Dieses Modul befasst sich mit häufig auftretenden Risiken wie Identitätsdiebstahl, betrügerische Transaktionen und Cyber-Bedrohungen. Es verdeutlicht die finanziellen und emotionalen Auswirkungen dieser Risiken auf Einzelpersonen und betont die Bedeutung des Schutzes persönlicher Informationen.

Das zweite Thema lautet „Sicher online einkaufen“. Die Hauptziele umfassen das Verständnis der Risiken beim Online-Shopping, die Identifizierung gängiger Methoden des Online-Betrugs und der Cyberkriminalität, die Bewertung der Sicherheit von Websites und Zahlungsmethoden sowie die Umsetzung von Strategien zum Schutz persönlicher und finanzieller Informationen. Die TeilnehmerInnen werden auch darin geschult, potenziellen Online-Betrug zu erkennen, um den persönlichen und gemeinschaftlichen Schutz zu verbessern.

Abschließend wird das Thema „Alternative Zahlungsmethoden“ vorgestellt, wobei verschiedene alternative Zahlungsmethoden wie E-Wallets, Kryptowährungen und mobile Zahlungen erläutert und analysiert werden. Es wird auch Wert darauf gelegt, die TeilnehmerInnen, insbesondere Frauen, über nachhaltige Zahlungsmethoden aufzuklären und sie zu befähigen, umwelt- und sozialverantwortliche finanzielle Entscheidungen zu treffen.

Insgesamt zielen diese Lernziele darauf ab, den TeilnehmerInnen ein umfassendes Verständnis der einzelnen Themen zu vermitteln und sie mit dem notwendigen Wissen und den Fähigkeiten auszustatten, um die Thematik effektiv zu bewältigen.

ONLINE SICHERHEIT

Identifizierung von gewöhnlichen Sicherheitsrisiken

Laut dem FBI tritt **Identitätsdiebstahl** dann auf, wenn jemand unrechtmäßig die persönlichen Informationen einer anderen Person (wie Name, Sozialversicherungsnummer, Kreditkartennummer oder Bankkontodetails) erlangt und verwendet, um Betrug oder andere Straftaten zu begehen.

Beispiele:

- Unbefugte Nutzung der Kreditkarten- oder Bankkontoinformationen einer anderen Person, um Einkäufe zu tätigen.
- Eröffnung neuer Kreditkonten oder Darlehen unter Verwendung der Identität einer anderen Person.
- Einreichung betrügerischer Steuererklärungen mit gestohlenen Sozialversicherungsnummern.

Betrügerische Transaktionen umfassen die unbefugte oder arglistige Erlangung, Nutzung oder Übertragung von Geldern, dem Eigentum oder anderen Vermögenswerten durch täuschende oder unehrliche Mittel.

Beispiele:

- Eine Betrügerin oder ein Betrüger, der sich als legitime Firmenvertretung ausgibt und Zahlungen für gefälschte Dienstleistungen oder Produkte fordert.
- Unbefugter Zugriff auf ein Bankkonto oder eine Kreditkarte, um unberechtigte Abhebungen oder Einkäufe zu tätigen.
- Falsche Rechnungsstellung oder Abrechnungsmethoden, bei denen Rechnungen für nie erbrachte Dienstleistungen versendet werden.

Cyber-Bedrohungen beziehen sich auf alle böswilligen Aktivitäten oder Ereignisse, die darauf abzielen, die Vertraulichkeit, Integrität oder Verfügbarkeit digitaler Informationen und Systeme zu gefährden.

Beispiele:

- Malware-Angriffe (z. B. Viren, Ransomware, Spyware), die Computersysteme oder Netzwerke infizieren und kompromittieren.
- Phishing-E-Mails oder Social-Engineering-Betrug, die darauf abzielen, Personen dazu zu bringen, sensible Informationen preiszugeben oder auf bösartige Links zu klicken.
- Datenlecks, bei denen unbefugte Parteien Zugriff auf sensible Informationen in Datenbanken oder auf Servern erhalten.

Wie können sich diese Risiken für den Einzelnen finanziell und emotional auswirken?

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

Finanzieller Schaden:

1. **Identitätsdiebstahl**: Die Opfer von Identitätsdiebstahl können erheblilche finanzielle Verluste durch unbefugte Transaktionen, betrügerische Kredite oder Belastungen auf ihren Konten erleiden. Sie können auch Kosten für Dienste zur Lösung von Identitätsdiebstahl und Anwaltsgebühren haben.
2. **Betrügerische Transaktionen**: Betroffene von betrügerischen Transaktionen können finanzielle Verluste in direkter Art & Weise erleiden, wenn Geld abgehoben oder unbefugte Belastungen auf ihren Konten vorgenommen werden. Indirekte finanzielle Auswirkungen können Überziehungsgebühren oder Gebühren für geplatzte Schecks umfassen.
3. **Cyber-Bedrohungen**: Die Opfer von Cyber-Bedrohungen können finanzielle Verluste erleiden, wenn ihre finanziellen Informationen gestohlen werden, Lösegeldzahlungen für den Zugang zu verschlüsselten Daten erforderlich sind oder Kosten für die Wiederherstellung nach Datenlecks anfallen, wie z.B. forensische Untersuchungen, regulatorische Geldstrafen oder Entschädigungen für Kunden.

Emotionaler Schaden:

1. **Identitätsdiebstahl**: Der emotionale Schaden durch Identitätsdiebstahl kann erheblich sein und Gefühle von Verletzung, Angst und Hilflosigkeit hervorrufen. Opfer können Stress und Frustration erleben, während sie den Diebstahl melden, betrügerische Belastungen bestreiten und ihre Identität wiederherstellen.
2. **Betrügerische Transaktionen**: Personen, die von betrügerischen Transaktionen betroffen sind, können Gefühle des Verrats und der Verwundbarkeit erfahren, insbesondere wenn der Betrug durch eine vertrauenswürdige Person begangen wurde. Sie können auch das Gefühl haben, die Kontrolle über ihre finanzielle Sicherheit und Privatsphäre verloren zu haben.
3. **Cyber-Bedrohungen**: Opfer von Cyber-Bedrohungen können Angst, Besorgnis und Misstrauen gegenüber der Sicherheit ihrer persönlichen Informationen und Online-Aktivitäten empfinden. Sie können auch ein Gefühl der Verwundbarkeit und Frustration über den wahrgenommenen Mangel an Kontrolle über ihre digitale Privatsphäre und Sicherheit haben.

Aktivität: Gruppendiskussion über kürzlich begangene Sicherheitsverletzungen und ihre Auswirkungen auf Einzelpersonen und Organisationen

Diese Aktivität zielt darauf ab, aktuelle Sicherheitsverletzungen und deren Auswirkungen auf Einzelpersonen und Organisationen zu analysieren und zu diskutieren. Zusätzlich sollen die finanziellen und emotionalen Folgen, die daraus gewonnenen Erkenntnisse und Präventionsstrategien erörtert werden.

Hier finden Sie eine Schritt-für-Schritt-Anleitung:

Teilen Sie die TeilnehmerInnen in kleine Gruppen von 4-6 Mitgliedern auf.

Weisen Sie jeder Gruppe eine aktuelle Fallstudie oder einen Nachrichtenartikel über eine Sicherheitsverletzung zur Analyse zu. Beispiele umfassen Datenlecks bei großen

Unternehmen, Ransomware-Angriffe auf Gesundheitsorganisationen oder Phishing-Betrug, die auf Einzelpersonen abzielen.

Die folgenden Beispiele können hierbei werden:

Datenlecks bei großen Unternehmen:

CAM4-Datenleck (März 2020): Die Elasticsearch-Datenbank der Adult-Video-Streaming-Website CAM4 wurde gehackt, wodurch über 10 Milliarden Datensätze offengelegt wurden. Zu den gestohlenen Daten gehörten vollständige Namen, E-Mail-Adressen, sexuelle Orientierung, Chat-Transkripte, E-Mail-Korrespondenz-Transkripte, Passwort-Hashes, IP-Adressen und Zahlungsprotokolle.

Yahoo-Datenleck (Oktober 2017): Yahoo gab bekannt, dass im August 2013 ein Datenleck 3 Milliarden Konten kompromittiert hatte. Der Vorfall wurde erstmals gemeldet, als Yahoo in Verhandlungen über den Verkauf an Verizon stand.

Aadhaar-Datenleck (März 2018): Die persönlichen Daten von mehr als einer Milliarde Bürger in Indien, die in der weltweit größten biometrischen Datenbank gespeichert sind, konnten online gekauft werden.

Ransomware-Angriffe auf Gesundheitsorganisationen:

University of Vermont (UVM) Medical Center (Oktober 2020): Mitarbeiter des UVM Medical Center konnten fast einen Monat lang keine elektronischen Gesundheitsakten (EHRs), Lohnabrechnungsprogramme und andere wichtige digitale Werkzeuge nutzen. Viele Operationen mussten verschoben werden, und Krebspatienten mussten zur Strahlenbehandlung woanders hingehen.

Inova Health System: Das Inova Health System war einer der Gesundheitsdienstleister, das Opfer eines Ransomware-Angriffs wurde.

Phishing-Betrug, die auf Einzelpersonen abzielen:

Spear-Phishing: Dies ist eine gezielte Phishing-Methode, bei der Cyberkriminelle Informationen stehlen, indem sie sich als vertrauenswürdige Quelle ausgeben.

HTTPS-Phishing: Ein Cyberkrimineller täuscht Sie, indem er eine bösartige Website verwendet, um Ihre persönlichen Informationen zu stehlen.

E-Mail-Phishing: Eine der häufigsten Phishing-Attacken ist das E-Mail-Phishing. Dabei sendet ein Cyberangreifer eine E-Mail, in der er vorgibt, jemand anderes zu sein, in der Hoffnung, dass Sie mit den angeforderten Informationen antworten.

Hier finden Sie eine Schritt-für-Schritt-Anleitung:

1. Teilen Sie die Teilnehmer in kleine Gruppen von 4-6 Mitgliedern auf.

2. Weisen Sie jeder Gruppe eine aktuelle Fallstudie oder einen Nachrichtenartikel über eine Sicherheitsverletzung zur Analyse zu. Die Beispiele beinhalten Datenlecks bei großen Unternehmen, Ransomware-Angriffe auf Gesundheitsorganisationen oder Phishing-Betrug, die auf Einzelpersonen abzielen.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

3. Geben Sie den Gruppen einige Leitfragen zur Diskussion vor:

- Was waren die Umstände und das Ausmaß der Sicherheitsverletzung?
- Wie hat der Vorfall Einzelpersonen und Organisationen finanziell und emotional betroffen?
- Welche wichtigen Erkenntnisse wurden aus dem Vorfall gewonnen?
- Welche Strategien oder Maßnahmen hätten zur Verhinderung der Sicherheitsverletzung beitragen können?

4. Geben Sie den Gruppen 20-30 Minuten Zeit, um die Fallstudie oder den Artikel zu überprüfen, die Fragen zu diskutieren und wichtigsten Punkte für die Präsentation vorzubereiten.

5. Treffen Sie sich nach der Diskussionszeit wieder als Gesamtgruppe.

6. Jede Gruppe präsentiert eine Zusammenfassung ihrer Erkenntnisse und hebt die wichtigsten Aspekte der Sicherheitsverletzung, deren Auswirkungen, gewonnene Erkenntnisse hervor.

7. Ermutigen Sie zu einer offenen Diskussion und zum Ideenaustausch unter den TeilnehmerInnen.

8. Führen Sie eine Nachbesprechung durch, bei der die TeilnehmerInnen über gemeinsame Themen, Herausforderungen und bewährte Verfahren aus den Fallstudien reflektieren.

9. Schließen Sie die Aktivität mit einer Zusammenfassung der wichtigsten Erkenntnisse ab und betonen Sie die Bedeutung des Bewusstseins für Cybersicherheit und proaktiver Maßnahmen zur Minderung von Sicherheitsrisiken.

Die Bedeutung von Sicherheitsmaßnahmen

Bevor wir uns in die Feinheiten der Online-Sicherheit vertiefen, nehmen wir uns einen Moment Zeit, um zu verstehen, warum es so wichtig ist, persönliche Informationen zu schützen. Persönliche Informationen, von Ihrem Namen bis zu Ihren Finanzdetails, spielen eine entscheidende Rolle in unserem Leben.

Sie umfassen eine Vielzahl von Daten, die dazu verwendet werden können, eine Person zu identifizieren oder zu lokalisieren. Dazu gehören unter anderem:

1. Name
2. Adresse
3. Sozialversicherungsnummer (SSN)
4. Geburtsdatum
5. E-Mail-Adresse
6. Telefonnummer
7. Finanzinformationen (z. B. Kreditkartennummern, Bankkontodaten)
8. Medizinische Informationen
9. Online-Kontozugangsdaten (z. B. Benutzernamen, Passwörter)

Den Schutz dieser Informationen zu gewährleisten, ist aus folgenden Gründen von entscheidender Bedeutung:

1. **Identitätsdiebstahl**: Eine der größten Risiken, die mit der Preisgabe persönlicher Informationen verbunden ist, verdeutlich sich im Identitätsdiebstahl. Identitätsdiebe können gestohlene persönliche Informationen verwenden, um betrügerische Konten zu eröffnen, unbefugte Einkäufe zu tätigen oder sogar Straftaten im Namen des Opfers zu begehen. Die finanziellen und emotionalen Auswirkungen von Identitätsdiebstahl können erheblich sein, da Opfer oft erhebliche Zeit und Ressourcen aufwenden, um Schaden zu verursachen.

2. **Finanzbetrug**: Dabei werden persönliche Informationen oft von Cyberkriminellen angegriffen, die finanziellen Betrug begehen wollen. Dies kann unbefugten Zugriff auf Bankkonten, Kreditkartenbetrug oder betrügerische Kreditanträge unter Verwendung gestohlener Identitäten umfassen. Die finanziellen Verluste aus einem solchem Betrug können verheerend sein und die Kreditwürdigkeit, finanzielle Stabilität und das Vertrauen der Finanzinstitute im Hinblick auf Einzelpersonen beeinträchtigen.

3. **Datenschutzverletzungen**: Der Schutz persönlicher Informationen ist entscheidend für den Schutz der Datenschutzrechte von Einzelpersonen. Unbefugter Zugriff auf persönliche Daten kann zu Datenschutzverletzungen führen, bei denen sensitive Informationen unbefugten Parteien preisgegeben werden. Datenschutzverletzungen können zu Peinlichkeiten, Rufschädigungen und einem Vertrauensverlust in Organisationen führen, die für den Schutz persönlicher Daten verantwortlich sind.

4. **Rechtliche und regulatorische Konsequenzen**: Organisationen, die es versäumen, persönliche Informationen angemessen zu schützen, können rechtliche und regulatorische Konsequenzen haben. Datenschutzgesetze wie die Datenschutz-Grundverordnung (DSGVO) in Europa oder der California Consumer Privacy Act (CCPA) in den Vereinigten Staaten stellen strenge Anforderungen an die Erhebung, Speicherung und Handhabung

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

personenbezogener Daten. Ein Verstoß gegen diese Vorschriften kann zu erheblichen Geldstrafen, rechtlichen Haftungen und Rufschädigungen für eine Organisation führen.

Praktiken zum Schutz persönlicher Informationen

Um die Sicherheit Ihrer persönlichen Informationen zu gewährleisten, befolgen Sie diese wesentlichen Schritte:

1. **Verwenden Sie starke Passwörter**: Erstellen Sie starke, einzigartige Passwörter für jedes Online-Konto und ändern Sie sie regelmäßig. Vermeiden Sie die Verwendung von leicht-erratbaren Passwörtern oder das Wiederverwenden von Passwörtern für mehrere Konten.

2. **Aktivieren Sie die Zwei-Faktor-Authentifizierung (2FA):** Wo immer möglich, aktivieren Sie die Zwei-Faktor-Authentifizierung, um Ihren Online-Konten zusätzliche Sicherheit zu verleihen. Die 2FA erfordert, dass Benutzer eine zweite Form der Verifizierung, wie einen Code, der an ihr Mobilgerät gesendet wird, zusätzlich zu ihrem Passwort überprüft.

3. **Seien Sie vorsichtig mit persönlichen Informationen:** Seien Sie vorsichtig beim Teilen persönlicher Informationen (Online oder am Telefon). Vermeiden Sie die Bereitstellung sensibler Informationen und überprüfen Sie die Legitimität von Anfragen, bevor Sie die Daten teilen.

4. **Sichern Sie Ihre Geräte:** Halten Sie Ihre Geräte, einschließlich Computer, Smartphones und Tablets in sicherer Verwahrung, indem Sie Antivirensoftware installieren, Firewalls aktivieren und Software mit den neuesten Sicherheitspatches aktualisieren.

5. **Bilden Sie sich weiter**: Informieren Sie sich über gängige Betrugsversuche und Phishing-Taktiken, die von Cyberkriminellen verwendet werden, um Personen dazu zu bringen, persönliche Informationen preiszugeben. Seien Sie wachsam und skeptisch gegenüber unaufgeforderten E-Mails, Telefonanrufen oder Nachrichten, die persönliche Informationen oder Zahlungen anfordern.

Überblick über die Sicherung von Online-Konten und Transaktionen zur Verhinderung unbefugten Zugriffs

In der heutigen digitalen Ära ist die Sicherheit von Online-Konten und Transaktionen von entscheidender Bedeutung, um sensible persönliche und finanzielle Informationen vor unbefugtem Zugriff und betrügerischen Aktivitäten zu schützen. Die Sicherung von Online-Konten und Transaktionen erfordert die Umsetzung einer Kombination aus präventiven Maßnahmen und bewährten Verfahren, um sich gegen verschiedene Cyber-Bedrohungen wie Hacking, Phishing und Identitätsdiebstahl zu schützen. Im Folgenden sind die wichtigsten Komponenten zur Sicherung von Online-Konten und Transaktionen aufgeführt:

Starke Passwörter:

1. Verwenden Sie für jedes Online-Konto starke und einzigartige Passwörter.
2. Vermeiden Sie leicht erratbare Passwörter wie "passwort123" oder "123456".
3. Erwägen Sie die Verwendung einer Passphrase, die aus einer Kombination von Buchstaben, Zahlen und Sonderzeichen besteht.
4. Aktualisieren Sie Passwörter regelmäßig und verwenden Sie sie nicht für mehrere Konten.

Zwei-Faktor-Authentifizierung (2FA):

1. Aktivieren Sie immer, wenn möglich, die Zwei-Faktor-Authentifizierung (2FA).
2. 2FA bietet eine zusätzliche Sicherheitsebene, indem Benutzer zur Bereitstellung einer zweiten Verifizierungsform aufgefordert werden, z. B. eines Codes, der an ihr Mobilgerät gesendet wird.
3. Dies hilft, unbefugten Zugriff zu verhindern, selbst wenn ein Passwort kompromittiert wird.

Sichere Kommunikation:

1. Stellen Sie sicher, dass Online-Transaktionen und -Kommunikationen über sichere Kanäle durchgeführt werden.
2. Achten Sie auf HTTPS in der Website-URL und ein Vorhängeschlosssymbol in der Browser-Adressleiste, das anzeigt, dass die Verbindung verschlüsselt ist.
3. Vermeiden Sie die Übertragung sensibler Informationen über ungesicherte Wi-Fi-Netzwerke, da diese möglicherweise anfällig für Interception durch Angreifer sind.

Regelmäßige Software-Updates:

1. Halten Sie Software, Betriebssysteme und Anwendungen mit den neuesten Sicherheitspatches und Updates auf dem neuesten Stand.
2. Schwachstellen in veralteter Software können von Angreifern ausgenutzt werden, um unbefugten Zugriff auf Geräte und Konten zu erhalten.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

Vorsicht vor Phishing-Angriffen:

1. Seien Sie vorsichtig bei Phishing-E-Mails, Texten oder Telefonanrufen, die versuchen, Benutzer dazu zu bringen, persönliche Informationen preiszugeben oder auf bösartige Links zu klicken.
2. Vermeiden Sie das Klicken auf Links oder das Herunterladen von Anhängen aus verdächtigen oder unaufgeforderten E-Mails.
3. Überprüfen Sie die Legitimität von Anfragen nach persönlichen Informationen, bevor Sie sensible Daten bereitstellen.

Verwendung sicherer Zahlungsmethoden:

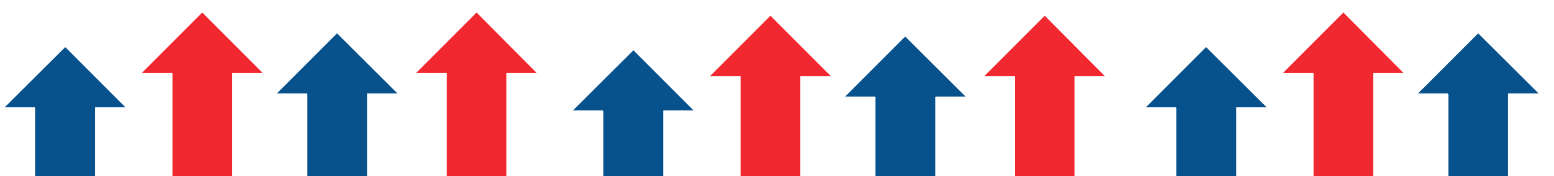
1. Verwenden Sie bei Online-Transaktionen sichere Zahlungsmethoden wie Kreditkarten oder seriöse Zahlungsplattformen, die einen Käuferschutz bieten.
2. Vermeiden Sie die Bereitstellung von Zahlungsinformationen an unsichere oder unbekannte Websites.

Überwachung der Kontenaktivität:

1. Überwachen Sie regelmäßig die Kontenaktivität und -auszüge auf unbefugte Transaktionen oder verdächtige Aktivitäten.
2. Melden Sie unbefugte Transaktionen oder verdächtige Aktivitäten sofort dem jeweiligen Finanzinstitut oder Diensteanbieter.

Datenverschlüsselung:

1. Verwenden Sie Verschlüsselungstechnologien zum Schutz sensibler Daten sowohl während der Übertragung als auch im Ruhezustand.
2. Die Verschlüsselung verändert die Daten so, um sie für unbefugte Benutzer unleserlich zu machen und damit den Daten-Diebstahl vorzubeugen.



Erklärung zur Erkennung und Vermeidung von Betrug zum Schutz vor finanziellen Verlusten

Betrug kann in verschiedenen Formen auftreten und damit Einzelpersonen über verschiedene Kanäle ansprechen (E-Mails, Telefonanrufe, Textnachrichten und Online-Werbung). Die Erkennung und Vermeidung von Betrug sind entscheidend, um sich vor finanziellen Verlusten und anderen negativen Folgen zu schützen.

Bilden Sie sich weiter:

1. Bleiben Sie über gängige Arten von Betrug und betrügerische Taktiken informiert, wie Phishing-Betrug, Anlagebetrug und Lotteriebetrug.
2. Seien Sie sich der neuesten Taktiken bewusst, die von Betrügern verwendet werden, um Einzelpersonen zu täuschen und ihr Vertrauen auszunutzen.

Seien Sie bei unaufgeforderter Kommunikation skeptisch:

1. Seien Sie vorsichtig bei unaufgeforderten E-Mails, Telefonanrufen oder Textnachrichten, die persönliche oder finanzielle Informationen anfordern.
2. Vermeiden Sie es, auf unaufgeforderte Kommunikationen zu antworten oder Links zu öffnen, insbesondere wenn sie verdächtig erscheinen oder zu gut klingen, um wahr zu sein.

Überprüfen Sie die Legitimität von Anfragen:

1. Überprüfen Sie die Legitimität von Anfragen nach persönlichen oder finanziellen Informationen, bevor Sie sensible Daten preisgeben.
2. Kontaktieren Sie die Organisation direkt über offiziell verfügbare Kontaktinformationen, um die Echtheit von Anfragen zu bestätigen.

Treffen Sie keine überstürzten Entscheidungen:

1. Vermeiden Sie es, überstürzte Entscheidungen zu treffen oder impulsiv auf Drucktaktiken von Betrügern zu reagieren.
2. Nehmen Sie sich Zeit, um Angebote oder Möglichkeiten zu recherchieren und zu überprüfen, bevor Sie finanzielle Verpflichtungen eingehen.

Schützen Sie persönliche Informationen:

1. Schützen Sie persönliche und finanzielle Informationen, indem Sie sensible Daten nicht mit unbekannten oder unverifizierten Parteien teilen.
2. Seien Sie vorsichtig beim Bereitstellen persönlicher Informationen. Insbesondere bei Websites, die nicht sicher oder vertrauenswürdig erscheinen.

Vertrauen Sie Ihren Instinkten:

1. Vertrauen Sie Ihren Instinkten und seien Sie misstrauisch gegenüber Angeboten oder Möglichkeiten, die zu gut erscheinen, um wahr zu sein.
2. Wenn etwas verdächtig erscheint oder nicht richtig zu sein scheint, ergreifen Sie die notwendigen Vorsichtsmaßnahmen und suchen Sie Rat bei vertrauenswürdigen Quellen.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

Aktivität: Rollenspiel, in dem die TeilnehmerInnen die Sicherung ihrer Online-Konten und Online-Transaktionen nachahmen.

Das Ziel dieser Rollenspielaktivität besteht darin, die TeilnehmerInnen in einem simulierten Szenario zu engagieren, in dem sie das Sichern ihrer Online-Konten und Transaktionen nachstellen. Durch aktive Teilnahme an der Rollenspielübung erhalten die TeilnehmerInnen praktische Erfahrungen, die richtigen Sicherheitsmaßnahmen zu implementieren, um unbefugten Zugriff auf ihre Online-Konten und Transaktionen zu verhindern.

Benötigte Materialien:

- Rollenspiel-Szenario-Prompts (im Voraus vorbereitet)
- Requisiten (optional)
- Schreibmaterialien

Anweisungen:

Einführung (5 Minuten):

- Erklären Sie den Zweck der Rollenspielaktivität: Die Sicherung der Online-Konten und Transaktionen, um unbefugten Zugriff zu verhindern.

- Erklären Sie, dass die TeilnehmerInnen in Paare oder kleine Gruppen aufgeteilt werden, um verschiedene Szenarien im Zusammenhang mit der Online-Sicherheit zu spielen.

Szenario-Zuweisung (5 Minuten):

- Teilen Sie die TeilnehmerInnen in Paare oder kleine Gruppen auf.

- Weisen Sie jedem Paar/Gruppe ein spezifisches Rollenspiel-Szenario zu, das sich mit dem Sichern von Online-Konten und Transaktionen befasst.

Mögliche Szenarien können sein:

- Erstellen eines starken Passworts und Aktivieren der Zwei-Faktor-Authentifizierung für ein E-Mail-Konto.

- Aktualisieren der Sicherheitseinstellungen für ein Online-Banking-Konto.

- Erkennen und Vermeiden von Phishing-Versuchen in einer E-Mail oder Textnachricht.

- Überprüfen der Legitimität einer Online-Shopping-Website vor einem Kauf.

Vorbereitung für das Rollenspiel (10 Minuten):

- Geben Sie den TeilnehmerInnen einen kurzen Überblick über ihr zugewiesenes Szenario, einschließlich der Ziele, die sie erreichen müssen, und etwaiger spezifischer Handlungen, die sie durchführen sollten.

Kurzüberblick:

a) Erstellen eines starken Passworts und Aktivieren der Zwei-Faktor-Authentifizierung für ein E-Mail-Konto: Die Teilnehmer simulieren den Prozess des Erstellens eines starken Passworts und der Aktivierung der Zwei-Faktor-Authentifizierung, um die Sicherheit eines E-Mail-Kontos zu verbessern. Diskutieren sie mögliche Strategien für die Erstellung eines sicheren Passworts und zusätzlicher Authentifizierungsmaßnahmen, um unbefugten Zugriff zu verhindern.

b) Aktualisieren der Sicherheitseinstellungen für ein Online-Banking-Konto: Die TeilnehmerInnen sollen die Schritte zum Aktualisieren der Sicherheitseinstellungen für ein Online-Banking-Konto durchspielen. Sie sollen die Datenschutzeinstellungen überprüfen und anpassen, Warnmeldungen für verdächtige Aktivitäten einrichten und zusätzliche Sicherheitsfunktionen der Online-Banking-Plattform erkunden.

c) Erkennen und Vermeiden von Phishing-Versuchen in einer E-Mail oder Textnachricht: Die TeilnehmerInnen werden mit einem Phishing-Versuch in einer E-Mail oder Textnachricht konfrontiert und sollen damit üben, die Warnsignale einer betrügerischen Kommunikation zu erkennen. Sie sollten Strategien diskutieren, um die Legitimität von Nachrichten zu überprüfen und potenziellen Betrug zu vermeiden.

d) Überprüfen der Legitimität einer Online-Shopping-Website vor einem Kauf: Die TeilnehmerInnen sollen die Legitimität einer Online-Shopping-Website überprüfen. Sie sollen die Sicherheitsfunktionen der Website, wie SSL-Verschlüsselung und sichere Zahlungsoptionen untersuchen und auf Basis dessen Strategien zur Identifizierung vertrauenswürdiger Online-Händler diskutieren.

Ermutigen Sie die TeilnehmerInnen dazu, gemeinsam zu brainstormen und ihren Ansatz für das Rollenspiel-Szenario zu planen. Sie sollten die Schritte diskutieren, die sie unternehmen werden, um ihre Online-Konten und Transaktionen effektiv zu sichern.

<u>Rollenspiel (20 Minuten):</u>

Die TeilnehmerInnen üben ihre zugewiesenen Szenarien und übernehmen dabei dir Rollen der beteiligten Personen (z. B. Kontoinhaber, Kundendienstmitarbeiter, Hacker).

Ermutigen Sie die TeilnehmerInnen, sich in realistischen Dialogen und Handlungen zu engagieren, während sie das Szenario durchlaufen und entsprechende Sicherheitsmaßnahmen implementieren, um unbefugten Zugriff zu verhindern.

Die Moderatoren können bei Bedarf eine entsprechende Anleitung und Unterstützung anbieten, Fragen beantworten und Vorschläge machen, um den TeilnehmerInnen zu einer effektiven Bewältigung der Übung zu ermutigen.

<u>Nachbesprechung und Diskussion (15 Minuten):</u>

Nach der Rollenspielaktivität versammeln Sie sich wieder als Gruppe zu einer Nachbesprechung und Diskussion.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

Bitten Sie die Teilnehmer, ihre Erfahrungen während der Rollenspielübung zu teilen, einschließlich etwaiger Herausforderungen, denen sie begegnet sind, und wie sie damit umgegangen sind.

Moderieren Sie eine Diskussion über die wichtigsten Erkenntnisse und Lektionen aus der Aktivität und betonen Sie die Bedeutung der Sicherung von Online-Konten und Transaktionen zur Verhinderung unbefugten Zugriffs.

Ermutigen Sie die TeilnehmerInnen, ihre eigenen Online-Sicherheitspraktiken zu reflektieren und Bereiche zur Verbesserung auf der Grundlage der Rollenspielszenarien zu identifizieren.

Abschluss (5 Minuten):

Fassen Sie die wichtigsten Punkte zusammen, die während der Aktivität diskutiert wurden und betonen Sie die Bedeutung proaktiver Online-Sicherheitsmaßnahmen.

Bedanken Sie sich bei den TeilnehmerInnen für ihre Teilnahme und Engagement bei der Rollenspielübung.

Grundlegende Sicherheitsmaßnahmen

Grundlegende Sicherheitsmaßnahmen bilden das Fundament einer robusten Verteidigung gegen digitale Bedrohungen. Die Verwendung von starken, einzigartigen Passwörtern, die Aktivierung der Zwei-Faktor-Authentifizierung (2FA) und regelmäßige Updates von Software und Geräten sind wesentliche Schritte zum Schutz Ihrer Online-Konten und persönlichen Informationen. In den folgenden Abschnitten werden wir tiefer in jede dieser Methoden eintauchen, ihre Bedeutung erläutern und praktische Tipps zur Umsetzung geben.

Bedeutung der Verwendung von starken, einzigartigen Passwörtern und Methoden zu ihrer Erstellung

In der heutigen digitalen Ära spielen Passwörter eine entscheidende Rolle beim Schutz unserer Online-Konten und sensiblen Informationen. Die Verbreitung von Cyberbedrohungen wie Phishing-Angriffen, Datenlecks und Brute-Force-Angriffen unterstreicht jedoch die Bedeutung der Verwendung von starken, einzigartigen Passwörtern. Hier sind mehrere Gründe, warum die Verwendung von starken und einzigartigen Passwörtern wichtig ist:

1. **Verhindern des unbefugten Zugriffs:** Starke, einzigartige Passwörter fungieren als erste Verteidigungslinie gegen unbefugten Zugriff auf unsere Online-Konten. Sie erschweren es Cyberkriminellen erheblich, Passwörter durch automatisierte Tools oder Brute-Force-Angriffe zu erraten oder zu knacken.

2. **Schutz persönlicher Informationen:** Online-Konten enthalten oft sensible persönliche und finanzielle Informationen wie Bankdaten, medizinische Aufzeichnungen und persönliche Kommunikationen. Die Verwendung von starken, einzigartigen Passwörtern hilft, diese Informationen vor unbefugtem

Zugriff zu schützen und verringert das Risiko von Identitätsdiebstahl, Finanzbetrug und Datenschutzverletzungen.

3. **Begrenzung der Auswirkungen von Datenlecks:** Im Falle eines Datenlecks, bei dem Anmeldeinformationen kompromittiert werden, können starke, einzigartige Passwörter für jedes Konto die Auswirkungen begrenzen, indem sie verhindern, dass Cyberkriminelle auf andere Konten mit denselben Anmeldeinformationen zugreifen. Diese Praxis, bekannt als Passworthygiene, trägt dazu bei, den Schaden zu begrenzen und die Exposition gegenüber weiteren Sicherheitsrisiken zu minimieren.

4. **Einhaltung bewährter Sicherheitspraktiken:** Starke, einzigartige Passwörter entsprechen bewährten Sicherheitspraktiken und den von Organisationen wie dem National Institute of Standards and Technology (NIST) und der Cybersecurity and Infrastructure Security Agency (CISA) empfohlenen Cybersicherheitsrichtlinien. Die Befolgung dieser Empfehlungen zeigt ein Engagement für die Online-Sicherheit und hilft Einzelpersonen und Organisationen, die relevanten Vorschriften und Standards einzuhalten.

Methoden zur Erstellung von starken, einzigartigen Passwörtern:

Die Erstellung von starken, einzigartigen Passwörtern erfordert die Verwendung einer Kombination von Zeichen, einschließlich Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen, um Passwörter widerstandsfähiger gegen Hacking-Versuche zu machen. Hier sind einige Methoden zur Erstellung von starken, einzigartigen Passwörtern:

1. **Passphrasen:** Anstatt traditionelle Passwörter zu verwenden, erwägen Sie die Verwendung von Passphrasen - längere Kombinationen von Wörtern oder Phrasen, die leicht zu merken, aber für andere schwer zu erraten sind. Passphrasen können aus zufälligen Wörtern, Liedtexten, Buchtiteln oder prägnanten Phrasen bestehen, die eine persönliche Bedeutung haben.

2. **Zufällige Zeichenkombinationen:** Verwenden Sie eine zufällige Kombination von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen, um ein einzigartiges Passwort zu erstellen. Vermeiden Sie leicht erratbare Muster oder Sequenzen wie "123456" oder "Passwort", die häufig von Hackern ins Visier genommen werden.

3. **Passwortgeneratoren:** Erwägen Sie die Verwendung von Passwortgenerator-Tools oder integrierten Funktionen in Passwortverwaltungssoftware, um starke, einzigartige Passwörter zu erstellen. Passwortgeneratoren können zufällige Passwörter unterschiedlicher Länge und Komplexität generieren, was sie äußerst sicher und schwer zu erraten macht.

4. **Vermeidung von Wörterbuch-Wörtern:** Vermeiden Sie die Verwendung von Wörtern direkt aus einem Wörterbuch oder leicht erratbaren Phrasen als Passwörter, da diese anfällig für Wörterbuchangriffe und Passwortknackwerkzeuge sind. Entscheiden Sie sich stattdessen für Kombinationen aus zufälligen Zeichen oder Passphrasen, die nicht in Wörterbüchern oder gängigen Sprachmustern zu finden sind.

5. **Einzigartige Passwörter für jedes Konto:** Stellen Sie sicher, dass jedes Online-Konto ein einzigartiges Passwort hat, um den Dominoeffekt eines einzelnen

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

kompromittierten Passworts zu verhindern, der zu unbefugtem Zugriff auf mehrere Konten führt. Vermeiden Sie die Verwendung desselben Passworts für mehrere Konten, da dies das Risiko von Sicherheitsverletzungen und Kompromissen erhöht.

Übersicht über die Zwei-Faktor-Authentifizierung und ihre Rolle bei der Verbesserung der Kontosicherheit

Die Zwei-Faktor-Authentifizierung (2FA) ist eine zusätzliche Sicherheitsebene, die verwendet wird, um Online-Konten über Benutzername und Passwort hinaus zu schützen. Sie erfordert, dass Benutzer zwei verschiedene Authentifizierungsfaktoren bereitstellen, um ihre Identität zu überprüfen und Zugang zu ihren Konten zu erhalten. Diese Authentifizierungsfaktoren fallen typischerweise in drei Kategorien: etwas, das Sie wissen (z. B. ein Passwort), etwas, das Sie haben (z. B. ein Mobilgerät oder Hardware-Token) und etwas, das Sie sind (z. B. biometrische Daten wie Fingerabdrücke oder Gesichtserkennung).

Bedeutung der Zwei-Faktor-Authentifizierung:

1. **Erhöhte Sicherheit:** Die 2FA verbessert die Kontosicherheit erheblich, indem eine zusätzliche Schutzebene über das Passwort hinaus hinzugefügt wird. Selbst wenn ein Hacker das Passwort eines Benutzers erlangt, benötigen sie immer noch Zugriff auf den zweiten Faktor (z. B. ein Mobilgerät oder biometrische Daten), um sich erfolgreich zu authentifizieren und Zugang zum Konto zu erhalten.

2. **Schutz vor Passwortdiebstahl**: Passwortdiebstahl ist eine gängige Methode, die von Hackern verwendet wird, um unbefugten Zugriff auf Online-Konten zu erlangen. Durch die Anforderung einer zweiten Authentifizierungsform verringert 2FA das Risiko eines unbefugten Zugriffs, auch wenn Passwörter kompromittiert sind.

3. **Reduziertes Risiko unbefugten Zugriffs:** 2FA verringert das Risiko unbefugten Zugriffs auf Konten, insbesondere im Falle von Passwortwiederverwendung oder schwachen Passwörtern. Selbst wenn das Passwort eines Benutzers aufgrund eines Datenlecks oder eines Phishing-Angriffs kompromittiert wird, fügt der zusätzliche Authentifizierungsfaktor eine weitere Sicherheitsebene hinzu.

4. **Einhaltung von Sicherheitsstandards:** Viele Organisationen und Regulierungsbehörden empfehlen oder verlangen die Verwendung von 2FA als Teil ihrer Sicherheitsprotokolle. Die Einhaltung dieser Standards trägt dazu bei, sicherzustellen, dass sensible Daten und Ressourcen angemessen vor unbefugtem Zugriff geschützt sind.

5. **Benutzerbewusstsein und -kontrolle:** 2FA verbessert das Benutzerbewusstsein und die Kontrolle über die Kontosicherheit, indem eine zusätzliche Verteidigungslinie gegen unbefugten Zugriff bereitgestellt wird. Benutzer sind in der Lage, proaktive Maßnahmen zu ergreifen, um ihre Konten und Daten zu schützen.

Methoden der Zwei-Faktor-Authentifizierung:

1. **Textnachricht (SMS)-Codes:** Ein Bestätigungscode wird per SMS an das Mobilgerät des Benutzers gesendet, den sie zusammen mit ihrem Passwort eingeben müssen, um sich zu authentifizieren.

2. **Authentifizierungs-Apps:** Benutzer können Authentifizierungs-Apps wie Google Authenticator, Microsoft Authenticator oder Authy auf ihren Mobilgeräten installieren. Diese Apps generieren zeitbasierte Einmalpasswörter (TOTPs), die Benutzer zusammen mit ihrem Passwort eingeben, um sich zu authentifizieren.

3. **Hardware-Token:** Einige Organisationen geben Hardware-Token aus, die Authentifizierungscodes generieren. Benutzer müssen das physische Token in ihrem Besitz haben, um sich zu authentifizieren.

4. **Biometrische Authentifizierung:** Einige Systeme unterstützen biometrische Authentifizierungsmethoden wie Fingerabdrücke, Gesichtserkennung oder Spracherkennung als zweiten Faktor.

Bedeutung regelmäßiger Aktualisierungen von Software und Geräten, um Sicherheitsschwachstellen zu beseitigen

Die Bedeutung regelmäßiger Updates von Software und Geräten zur Minimierung von Sicherheitslücken kann nicht genug betont werden. Hier sind einige wichtige Gründe, warum dies entscheidend ist:

1. **Behebung von Sicherheitslücken:** Software-Updates enthalten oft Patches, die bekannte Sicherheitslücken adressieren. Diese Lücken können von Cyberkriminellen ausgenutzt werden, um unbefugten Zugriff auf Systeme zu erlangen, sensible Informationen zu stehlen oder Dienste zu stören. Regelmäßige Updates stellen damit sicher, dass diese Schwachstellen zeitnah behoben werden und das Risiko von Ausnutzung reduziert wird.

2. **Schutz vor Exploits:** Cyberkriminelle entwickeln ständig neue Techniken und Exploits, um Software und Geräte anzugreifen. Durch das ständige Aktualisieren von Software und Geräten auf dem neuesten Stand können sich Benutzer vor neu entdeckten Schwachstellen und Exploits schützen. Dies trägt zur Integrität und Sicherheit von Systemen und Daten bei.

3. **Einhaltung von Vorschriften:** In vielen Branchen ist die Einhaltung von Vorschriften und Standards im Bereich der Cybersicherheit obligatorisch. Die regelmäßige Aktualisierung von Software und Geräten ist oft eine Anforderung dieser Vorschriften und Standards. Die Nichteinhaltung dieser Anforderungen kann zu Strafen, Geldbußen oder anderen rechtlichen Konsequenzen führen.

4. **Verbesserung von Stabilität und Leistung:** Software-Updates adressieren nicht nur Sicherheitslücken, sondern enthalten auch Verbesserungen der Stabilität und Leistung. Durch das Halten von Software und Geräten auf dem neuesten Stand können Benutzer von erhöhter Zuverlässigkeit, schnellerer Leistung und verbesserter Funktionalität profitieren.

5. **Schutz vor Malware und Cyberangriffen:** Veraltete Software und Geräte sind anfälliger für Malware-Infektionen und Cyberangriffe. Cyberkriminelle nutzen oft bekannte Schwachstellen in veralteter Software aus, um Malware wie Ransomware, Viren oder Spyware zu verbreiten. Regelmäßige Updates schützen vor diesen Bedrohungen.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

6. **Aufrechterhaltung des Herstellersupports:** Softwarehersteller bieten in der Regel für einen begrenzten Zeitraum Unterstützung und Wartung für ihre Produkte an. Wenn Software das Ende ihres Supportlebenszyklus erreicht, können Hersteller damit aufhören, Updates und Patches zu veröffentlichen, wodurch Benutzer anfällig für Sicherheitsbedrohungen werden. Durch regelmäßige Updates von Software und Geräten stellen Benutzer sicher, dass sie weiterhin Herstellersupport und Schutz vor Sicherheitslücken erhalten.

Aktivität: Praktischer Workshop zur Erstellung sicherer Passwörter und zur Aktivierung der Zwei-Faktor-Authentifizierung auf verschiedenen Online-Plattformen.

Das Ziel dieses Workshops ist es, die Teilnehmer über die Bedeutung der Erstellung starker Passwörter und der Aktivierung der Zwei-Faktor-Authentifizierung (2FA) zu informieren, um die Sicherheit ihrer Online-Konten zu verbessern. Die TeilnehmerInnen sollen dabei erlernen, wie sie starke Passwörter erstellen sowie die 2FA auf verschiedenen Online-Plattformen einrichten können.

Benötigte Materialien:

Computer oder mobile Geräte mit Internetzugang für jede/n TeilnehmerIn

Präsentationsfolien oder Handouts zur Erstellung starker Passwörter und zur Aktivierung der 2FA

Beispiele für Online-Plattformen, die 2FA unterstützen (z. B. Google, Facebook, Twitter, Bankwebsites)

Schreibmaterialien

Anweisungen:

Einführung (10 Minuten):

Begrüßen Sie die TeilnehmerInnen des Workshops und erläutern Sie die Bedeutung der Erstellung starker Passwörter und der Aktivierung der Zwei-Faktor-Authentifizierung (2FA) zur Verbesserung der Online-Sicherheit.

Geben Sie einen Überblick über die Agenda des Workshops und den entsprechenden Lernzielen.

Präsentation zur Erstellung starker Passwörter (15 Minuten):

Geben Sie einen kurzen Überblick über die Merkmale starker Passwörter, einschließlich Länge, Komplexität und Einzigartigkeit.

Geben Sie Tipps und Richtlinien zur Erstellung starker Passwörter, wie die Verwendung einer Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.

Demonstrieren Sie Techniken zum Passwortmanagement, wie die Verwendung von Passwortmanagern zur sicheren Generierung und Speicherung starker Passwörter.

Zum Beispiel:

1Password: Bekannt für seine unschlagbare Sicherheit und zahlreiche zusätzliche Funktionen. Es ist die erste Wahl für die meisten Benutzer und besonders gut für Familien geeignet.

Dashlane: Bietet herausragende Extras wie Überwachung des Darknets und einen schnellen VPN-Dienst. Es ist auch bekannt für sein Premium-Passwortmanagement.

RoboForm: Ein erschwinglicher Passwortmanager mit guter Sicherheit und leistungsstarken Formularausfüllfunktionen.

Keeper: Hochsicherer Passwortmanager mit intuitiven Apps und flexiblen Preisen.

NordPass: Bekannt für sein sicheres Passwortmanagement und besonders geeignet für Administratoren von Unternehmenskonten.

Bitwarden: Bekannt für sein kostenloses Passwortmanagement.

Diese Passwortmanager können Ihnen helfen, einzigartige und starke Passwörter für jeden Ihrer Online-Accounts zu erstellen und Sie über potenzielle Datenlecks zu informieren. Sie sind alle entweder vollständig kostenlos oder sehr kostengünstig. Bitte beachten Sie, dass diese Passwortmanager zwar ähnliche Dienste anbieten, sich die genauen Funktionen und Preise jedoch unterscheiden können. Es ist immer eine gute Idee, die offiziellen Websites für die genauesten und aktuellen Informationen zu besuchen.

Hands-on-Aktivität: Erstellung starker Passwörter (20 Minuten):

Teilen Sie die Teilnehmer zu Paaren oder kleine Gruppen auf.

Geben Sie den TeilnehmerInnen eine Liste gängiger Online-Konten (z.B. E-Mail, soziale Medien, Bankwesen) und bitten Sie sie, für jedes Konto starke Passwörter zu erstellen.

Ermutigen Sie die TeilnehmerInnen, die zuvor besprochenen Richtlinien zur Passworterstellung anzuwenden und sicherzustellen, dass jedes Passwort einzigartig und nicht leicht zu erraten ist.

Unterstützten Sie die einzelnen Gruppen, sofern notwendig.

Präsentation zur Aktivierung der Zwei-Faktor-Authentifizierung (2FA) (15 Minuten):

Geben Sie einen Überblick über die Zwei-Faktor-Authentifizierung (2FA) und ihre Rolle bei der Verbesserung der Sicherheit von Online-Konten.

Erklären Sie die verschiedenen Arten von 2FA-Methoden, wie SMS-Codes, Authentifizierungs-Apps und Hardware-Token.

Geben Sie eine schrittweise Anleitung zur Aktivierung von 2FA auf verschiedenen Online-Plattformen vor.

Hands-on-Aktivität: Aktivierung der Zwei-Faktor-Authentifizierung (2FA) (20 Minuten):

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

Weisen Sie die Teilnehmerinnen an, eine Online-Plattform auszuwählen, die 2FA unterstützt (z.B. Google, Facebook, Twitter, Bankwebsite).

Führen Sie die TeilnehmerInnen durch den Prozess der Aktivierung der 2FA auf ihrer gewählten Plattform, unter Verwendung der bereitgestellten schrittweisen Anweisungen.

Ermutigen Sie die TeilnehmerInnen, ihre mobilen Geräte oder Computer zu verwenden, um den Anweisungen zu folgen und die 2FA auf ihren Konten zu aktivieren.

Bieten Sie Unterstützung an, falls erforderlich.

Abschluss und Diskussion (10 Minuten):

Versammeln Sie die TeilnehmerInnen für eine kurze Abschluss- und Diskussionsrunde.

Überprüfen Sie die wichtigsten Erkenntnisse aus dem Workshop, einschließlich der Bedeutung der Erstellung starker Passwörter und der Aktivierung der Zwei-Faktor-Authentifizierung (2FA) zur Verbesserung der Online-Sicherheit.

Ermutigen Sie die TeilnehmerInnen, ihre Erfahrungen und eventuelle Herausforderungen während der praktischen Übungen zu teilen.

Bieten Sie zusätzliche Ressourcen und Unterstützung für TeilnehmerInnen an, die mehr über bewährte Verfahren zur Online-Sicherheit erfahren möchten.

Fazit:

Bedanken Sie sich bei den TeilnehmerInnen für die Teilnahme und das Engagement im Workshop.

Erinnern Sie die TeilnehmerInnen daran, das Wissen und die Fähigkeiten, die sie erworben haben, anzuwenden, um zukünftig ihre Online-Konten zu sichern und ihre persönlichen Informationen zu schützen.

Ermutigen Sie die TeilnehmerInnen dazu, ihr neues Wissen mit Freunden, der Familie und KollegInnen zu teilen, um bessere Praktiken für die Online-Sicherheit zu fördern.

Erkennen des Betrugs

Im Folgenden werden gängige Arten von Betrugsversuchen sowie deren Merkmale und Warnsignale untersucht.

Phishing-E-Mails sind betrügerische E-Mails, die vorgeben, von legitimen Organisationen oder Personen zu stammen, die jedoch darauf abzielen, Empfänger dazu zu bringen, sensible Informationen preiszugeben. Dies umfasst Passwörter, Benutzernamen, Kreditkartennummern oder andere persönliche Daten. Diese E-Mails enthalten oft Links zu gefälschten Websites oder bösartigen Anhängen.

Beispiel: Im Jahr 2016 wurde eine weit verbreitete Phishing-Attacke auf Gmail-Nutzer gestartet, indem E-Mails versendet wurden, die von Google zu stammen schienen und Benutzer aufforderten, auf einen Link zu einer gefälschten Google-Login-Seite zu klicken. Benutzer, die ihre Anmeldeinformationen auf der gefälschten Seite eingaben, gaben versehentlich ihre Anmeldeinformationen an die Angreifer bekannt, die dann unbefugten Zugriff auf ihre Konten erlangten.

Ponzi-Systeme sind betrügerische Anlagepläne, die Investoren hohe Renditen bei wenig oder keinem Risiko versprechen. In einem Ponzi-System werden frühe Investoren anstelle aus legitimen Gewinnen, aus den Investitionen späterer Investoren bezahlt. Wenn das System wächst, kann der Betreiber Gelder von neuen Investoren verwenden, um Renditen an frühere Investoren zu zahlen und so die Illusion der Rentabilität zu erzeugen.

Beispiel: Eines der berüchtigtsten Ponzi-Systeme der Geschichte wurde von Bernie Madoff inszeniert, der über mehrere Jahrzehnte Investoren um Milliarden von Dollar betrog. Madoff versprach den Investoren durch seine Investmentfirma konstante, hohe Renditen, verwendete jedoch stattdessen die Gelder neuer Investoren, um Renditen an bestehende Investoren zu zahlen. Das System brach schließlich 2008 zusammen und führte zu massiven finanziellen Verlusten für Tausende von Anlegern.

Anlagebetrug umfasst betrügerische Pläne oder Angebote, die hohe Renditen bei Investitionen versprechen, letztendlich jedoch zu finanziellen Verlusten für die Anleger führen. Diese Betrugsversuche zielen oft auf Einzelpersonen ab, die ihr Geld in scheinbar „zu gute“ Angebote investieren möchten.

Beispiel: In den letzten Jahren ist Kryptowährungsanlage-Betrug immer häufiger geworden. Betrüger können gefälschte Initial Coin Offerings (ICOs) oder Anlagechancen in gefälschte Kryptowährungen bewerben, die hohe Renditen bei minimalem Risiko versprechen. Diese Betrugsversuche sind darauf ausgelegt, Investoren dazu zu bringen, ihr Geld an die Betrüger zu senden, was zu finanziellen Verlusten für die Opfer führt.

Merkmale und Warnhinweise der Betrugsarten

1. Phishing-E-Mails:

Merkmale:

1. Phishing-E-Mails erscheinen oft von legitimen Organisationen wie Banken, sozialen Medienplattformen oder Regierungsbehörden zu stammen.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

2. Sie enthalten typischerweise dringende oder alarmierende Nachrichten, die Empfänger dazu veranlassen, sofort zu handeln, wie das Klicken auf einen Link oder die Bereitstellung sensibler Informationen.
3. Phishing-E-Mails können gefälschte Logos, Marken oder E-Mail-Adressen enthalten, die legitime Quellen imitieren, um Empfänger zu täuschen.

Warnsignale, auf die zu achten ist:

1. **Allgemeine Begrüßungen**: Phishing-E-Mails verwenden oft allgemeine Begrüßungen wie "Sehr geehrter Kunde", anstatt Empfänger mit ihrem Namen anzusprechen.
2. **Dringende Anfragen**: Phishing-E-Mails können dringende Anfragen nach persönlichen Informationen, Kontoverifizierung oder sofortiger Handlung enthalten, um Konsequenzen zu vermeiden.
3. **Verdächtige Links**: Seien Sie misstrauisch gegenüber Links in E-Mails, die Sie zu unbekannten Websites oder URLs führen, die nicht mit der Domain des Absenders übereinstimmen.
4. **Schlechte Grammatik und Rechtschreibung**: Phishing-E-Mails enthalten oft Rechtschreib- und Grammatikfehler, ungewöhnliche Formatierungen oder ungeschickte Sprache, die darauf hindeuten können, dass sie nicht von einer legitimen Quelle stammen.
5. **Anfragen nach persönlichen Informationen**: Seriöse Organisationen fordern in der Regel keine sensiblen Informationen wie Passwörter, Sozialversicherungsnummern oder Kontodetails per E-Mail an.

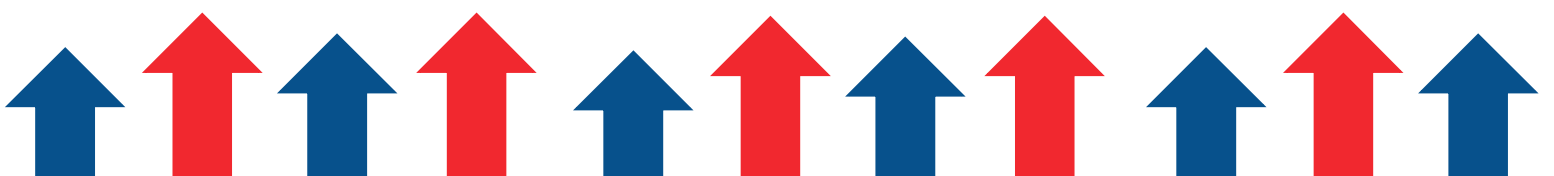
2. Ponzi Systeme:

Merkmale:

1. Ponzi-Systeme versprechen hohe Renditen bei minimalen Risiken.
2. Sie verlassen sich auf einen kontinuierlichen Zustrom neuer Investoren, um Renditen an bestehende Investoren zu zahlen, anstatt legitime Gewinne aus Investitionen zu generieren.
3. Ponzi-Systeme verwenden oft komplexe Anlagestrategien oder einen komplizierten Finanzjargon, um Investoren zu verwirren und die Illusion der Legitimität zu erzeugen.

Warnsignale, auf die zu achten ist:

1. **Unrealistische Renditen**: Seien Sie vorsichtig bei Investitionsmöglichkeiten, die kontinuierlich hohe Renditen bei geringem oder keinem Risiko versprechen.
2. **Mangelnde Transparenz**: Ponzi-Systeme weisen oft eine mangelnde Transparenz darüber auf, wie Investorengelder verwendet oder investiert werden.
3. **Druck zum Investieren:** Betrüger können Hochdruckverkaufstaktiken verwenden, um Einzelpersonen schnell zu überzeugen, ohne ausreichend Zeit für eine Due Diligence oder Recherche zu bieten.
4. **Keine Registrierung oder Regulierung:** Seriöse Investitionsmöglichkeiten sind in der Regel bei Regulierungsbehörden registriert und unterliegen einer Aufsicht. Ponzi-Systeme können keine ordnungsgemäße Registrierung oder Regulierung aufweisen.



3. Investitionsbetrug:

Merkmale:

1. Investitionsbetrug können betrügerische Angebote oder Möglichkeiten im Zusammenhang mit Aktien, Immobilien, Kryptowährungen oder anderen Finanzprodukten umfassen.
2. Betrüger können falsche oder irreführende Informationen verwenden, um Einzelpersonen dazu zu verleiten, Geld zu investieren.
3. Investitionsbetrug versprechen oft hohe Renditen mit minimalem Aufwand oder Risiko und spielen auf den Wunsch von Einzelpersonen nach schnellen Gewinnen an.

Warnsignale, auf die zu achten ist:

1. **Unaufgeforderte Angebote**: Seien Sie vorsichtig bei unaufgeforderten Investitionsangeboten per E-Mail, Telefonanrufen, sozialen Medien oder Online-Werbung.
2. **Fehlende Dokumentation**: Seriöse Investitionsmöglichkeiten bieten in der Regel Dokumentations- oder Offenlegungsmaterialien, die die Anlagebedingungen, Risiken und Bedingungen detailliert erläutern. Seien Sie misstrauisch gegenüber Möglichkeiten, die keine ordnungsgemäße Dokumentation oder Transparenz aufweisen.
3. **Druck zum schnellen Handeln**: Betrüger können Einzelpersonen unter Druck setzen, schnell Investitionsentscheidungen zu treffen, ohne ausreichend Zeit für Due Diligence oder Recherche zu bieten.
4. **Garantierte Renditen**: Seien Sie skeptisch gegenüber Investitionsmöglichkeiten, die hohe Renditen garantieren oder minimales Risiko versprechen. Alle Investitionen bergen ein gewisses Risiko. Seriöse Investitionsmöglichkeiten garantieren keine Gewinne.

Aktivität: Analyse von Phishing-E-Mails und Identifizierung von Schlüsselelementen, die auf einen Betrug hinweisen

Das Ziel dieser Aktivität ist es, die TeilnehmerInnen über die wichtigsten Elemente von Phishing-E-Mails aufzuklären und ihnen beizubringen, sie als betrügerisch zu identifizieren. Die Teilnehmer werden echte Phishing-E-Mails analysieren und die Warnsignale identifizieren, die darauf hinweisen, dass es sich um Betrug handelt.

Benötigte Materialien:

1. Ausdrucke oder digitale Kopien von echten Phishing-E-Mails (stellen Sie sicher, dass diese E-Mails keine bösartigen Links oder Anhänge enthalten)
2. Whiteboard oder Flipchart
3. Schreibmaterialien

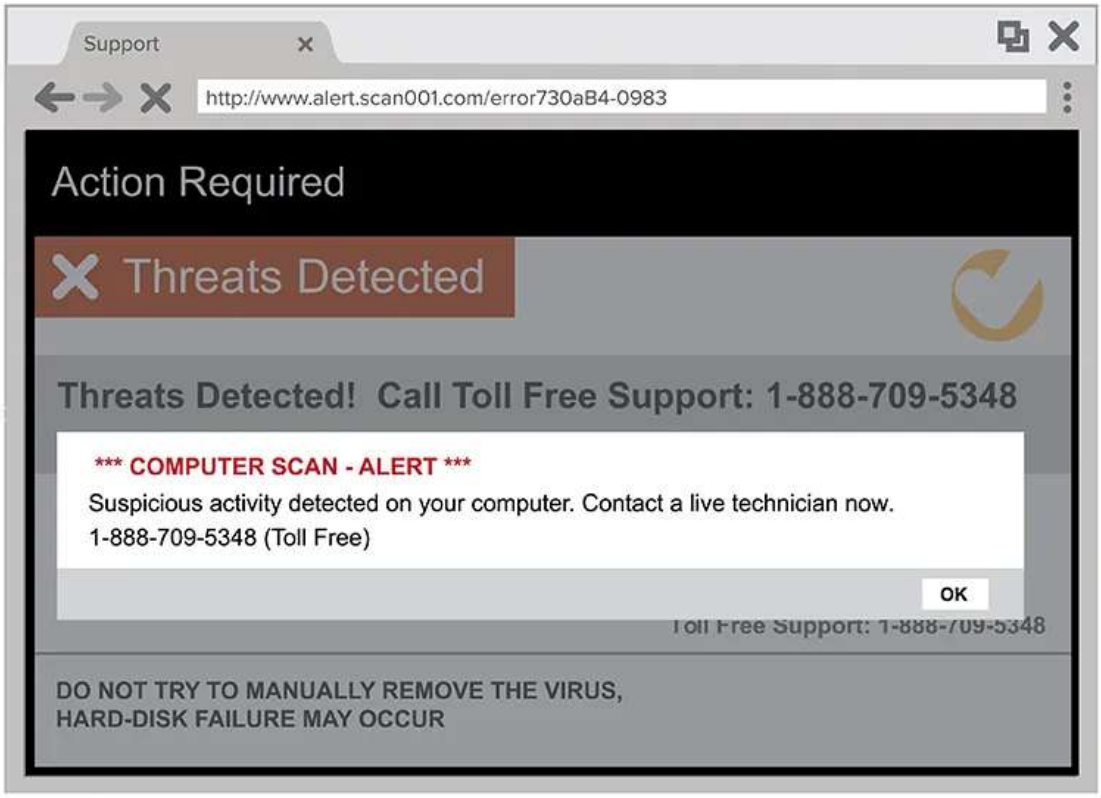
Examples:

1. Phishing-E-Mails im Bereich Technischer Support

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

Mit Einschüchterungstaktiken in E-Mails und Pop-ups täuschen Betrüger Opfer, indem sie ihnen vorgaukeln, dass sie technischen Support benötigen. Die Betrüger könnten sich als Microsoft ausgeben — die am häufigsten gefälschte Marke im Jahr 2023 [*] — oder als Best Buy's Geek Squad, um Sie davon zu überzeugen, dass es ein Problem mit Ihrem Gerät gibt.

Wie Technischer-Support-Betrug funktionieren:

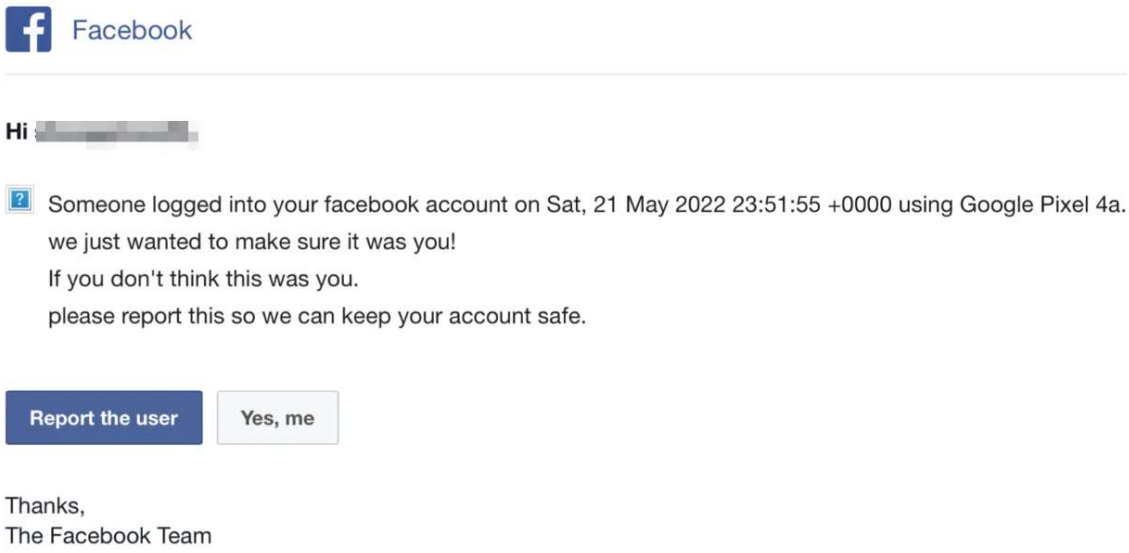


- Betrüger verwenden hochtechnische oder vage Cybersecurity-Begriffe, um Sie zu verängstigen, zu verwirren und zu entwaffnen.
- Sie können Ihnen für erfundene Geräte- oder Software-Reparaturen Rechnungen stellen — oder Sie zu unnötigen Upgrades oder Garantieverlängerungen überreden.
- Sie könnten Sie dazu drängen, auf bösartige Anhänge zu klicken oder eine Website zu besuchen, um Ihre Informationen preiszugeben.
- Sie könnten um Fernzugriff auf Ihren Computer bitten, um angebliche Probleme zu beheben, was es ihnen ermöglicht, Malware oder Ransomware zu installieren.

Phishing-E-Mails in sozialen Medien

Bei diesem Betrug stammt die Phishing-E-Mail angeblich von einem Support-Team eines sozialen Netzwerks wie Instagram oder LinkedIn. Die Nachricht ahmt eine typische Warnung oder Benachrichtigung über das Konto nach, um authentisch zu erscheinen und Ihre Aufmerksamkeit zu erregen.

Eine gefälschte E-Mail-Benachrichtigung über eine Anmeldung, die eine Facebook-Seite imitiert, mit einer entsprechenden Handlungsaufforderung (CTA) zum "Melden des Benutzers".



Beispiel für einen Phishing-Betrug in den sozialen Medien. Quelle: Reddit.

Wie Social-Media-Phishing-Betrug funktioniert:

- Diese betrügerische E-Mail enthält einen Phishing-Link, um Ihr Konto zu verifizieren oder sich anzumelden.
- Wenn Sie auf den Link klicken, kann dies Malware oder Spyware herunterladen oder Sie zu einer gefälschten Anmeldeseite führen.
- Sobald die Betrüger Ihre Kontoinformationen haben, können sie sich anmelden und Sie aussperren oder sich an anderer Stelle anmelden, wenn Sie Ihr Passwort wiederverwendet haben.

Anleitung:

Einführung (5 Minuten):

Begrüßen Sie die Teilnehmer zur Aktivität und erklären Sie den Zweck: die Analyse von Phishing-E-Mails und die Identifizierung von Schlüsselelementen, die darauf hinweisen, dass sie betrügerisch sind.

Geben Sie einen Überblick über Phishing-E-Mails und die Bedeutung, sie erkennen zu können, um sich vor Cyberbedrohungen zu schützen.

Präsentation zu Schlüsselelementen von Phishing-E-Mails (10 Minuten):

Geben Sie einen kurzen Überblick über die Schlüsselelemente von Phishing-E-Mails, einschließlich gemeinsamer Merkmale und Warnsignale.

Diskutieren Sie Elemente wie allgemeine Begrüßungen, dringende Anfragen, verdächtige Links oder Anhänge, schlechte Grammatik und Rechtschreibung sowie Anfragen nach persönlichen Informationen.

Analyse von Phishing-E-Mails (30 Minuten):

Teilen Sie die TeilnehmerInnen in kleine Gruppen auf.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

Verteilen Sie Ausdrucke oder zeigen Sie digitale Kopien echter Phishing-E-Mails für jede Gruppe zur Analyse.

Weisen Sie die TeilnehmerInnen an, die Phishing-E-Mails sorgfältig zu untersuchen und Schlüsselelemente zu identifizieren, die darauf hinweisen, dass sie betrügerisch sind.

Ermutigen Sie die TeilnehmerInnen dazu, ihre Erkenntnisse innerhalb ihrer Gruppen zu diskutieren und die identifizierten Warnsignale festzuhalten.

Gruppendiskussion (15 Minuten):

Kommen Sie als Gesamtgruppe wieder zusammen und bitten Sie jede Gruppe, ihre Beobachtungen und Ergebnisse aus der Analyse der Phishing-E-Mails zu teilen.

Leiten Sie eine Diskussion über die häufigsten Warnsignale und Schlüsselelemente von Phishing-E-Mails ein, die von den TeilnehmerInnen identifiziert wurden.

Verwenden Sie ein Whiteboard oder Flipchart, um die von den TeilnehmerInnen identifizierten Warnsignale und Schlüsselelemente zu dokumentieren.

Reflexion und Erkenntnisse (10 Minuten):

Leiten Sie eine Reflexionssitzung ein, in der die TeilnehmerInnen ihre Gedanken und Erkenntnisse aus der Analyse von Phishing-E-Mails reflektieren.

Diskutieren Sie Strategien zum Schutz vor Phishing-Angriffen, wie das Überprüfen von Absender-E-Mail-Adressen, das Vermeiden des Klickens auf verdächtige Links oder Anhänge und das Melden von Phishing-Versuchen an die entsprechenden Behörden.

Fassen Sie die wichtigsten Erkenntnisse zusammen und betonen Sie die Bedeutung von Wachsamkeit und Skepsis im Umgang mit unaufgeforderten E-Mails.

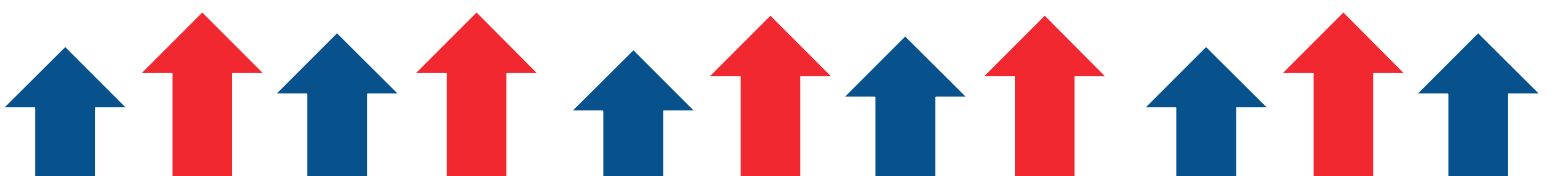
Abschluss:

Bedanken Sie sich bei den TeilnehmerInnen für ihre Teilnahme an der Aktivität und ihre Beiträge zur Diskussion.

Ermutigen Sie die TeilnehmerInnen, die erworbenen Kenntnisse und Fähigkeiten anzuwenden, um Phishing-E-Mails in ihrem privaten und beruflichen Leben zu identifizieren und sich dagegen zu schützen.

Die Bedeutung des Cybersecurity-Bewusstseins

Die Sensibilisierung für Cybersicherheit ist entscheidend, um sich vor verschiedenen Online-Bedrohungen zu schützen. Das Verständnis für die von Cyberkriminellen angewandten Strategien zur Täuschung von Einzelpersonen, wie etwa Phishing-Versuche, ist entscheidend für die Aufrechterhaltung der digitalen Sicherheit. Durch das Erkennen gängiger Phishing-Taktiken und das zum Unterschied von legitimen E-Mails können Einzelpersonen die Risiken eines Cyberangriffs minimieren.



Strategien zur Erkennung von Phishing-Versuchen und zur Unterscheidung von legitimen E-Mails

Phishing-Versuche zielen oft darauf ab, Empfänger dazu zu bringen, sensible Informationen preiszugeben oder auf bösartige Links zu klicken. Durch die Anwendung der folgenden Strategien können Einzelpersonen ihre Fähigkeit verbessern, Phishing-Versuche zu erkennen und zu vereiteln:

Überprüfen der E-Mail-Adresse des Absenders: Überprüfen Sie die E-Mail-Adresse des Absenders, um sicherzustellen, dass sie mit der offiziellen Domain der Organisation oder Person übereinstimmt. Seien Sie vorsichtig bei E-Mail-Adressen, die falsch geschriebene oder verdächtige Domainnamen verwenden.

Überprüfen von allgemeinen Begrüßungen: Phishing-E-Mails verwenden oft allgemeine Begrüßungen wie "Sehr geehrter Kunde" oder "Sehr geehrter Benutzer", anstatt die Empfänger mit ihrem Namen anzusprechen. Seriöse E-Mails von renommierten Organisationen adressieren Empfänger normalerweise mit ihrem Namen.

Achten auf dringende Anfragen oder Drohungen: Phishing-E-Mails enthalten oft dringende Anfragen oder Drohungen, die darauf abzielen, ein Gefühl der Dringlichkeit zu erzeugen und die Empfänger unter Druck zu setzen, sofort zu handeln. Seien Sie vorsichtig bei E-Mails, die mit Konsequenzen drohen, wenn Sie nicht schnell reagieren oder persönliche Informationen bereitstellen.

Überprüfen von Links und URLs: Bewegen Sie den Mauszeiger über Hyperlinks in E-Mails (ohne zu klicken), um die Ziel-URL zu sehen. Überprüfen Sie, ob die URL mit der offiziellen Website der behaupteten Organisation übereinstimmt. Seien Sie vorsichtig bei verkürzten URLs oder Links, die zu unbekannten oder verdächtigen Websites weiterleiten.

Vermeiden Sie das Öffnen von Anhängen: Seien Sie vorsichtig bei E-Mail-Anhängen, insbesondere wenn sie von unbekannten oder unerwarteten Quellen stammen. Phishing-E-Mails können bösartige Anhänge enthalten, die Malware auf Ihrem Gerät installieren oder Ihre Sicherheit gefährden können.

Überprüfen von Anfragen nach persönlichen Informationen: Seien Sie skeptisch gegenüber E-Mails, die sensible Informationen wie Passwörter, Sozialversicherungsnummern, Kreditkartendaten oder Kontodaten anfordern. Seriöse Organisationen fordern in der Regel keine sensiblen Informationen per E-Mail an.

Überprüfen von Rechtschreib- und Grammatikfehlern: Phishing-E-Mails enthalten oft Rechtschreib- und Grammatikfehler, ungewöhnliche Satzstruktur oder ungeschickte Sprache, die darauf hinweisen können, dass sie nicht von einer legitimen Quelle stammen. Seien Sie misstrauisch gegenüber E-Mails mit schlechter sprachlicher Qualität.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

Seien Sie vorsichtig bei ungewöhnlichen Anfragen oder Angeboten: Seien Sie skeptisch gegenüber E-Mails, die unerwartete Belohnungen, Preise oder Angebote anbieten, die zu gut erscheinen, um wahr zu sein. Phishing-E-Mails können auch Empfänger auffordern, an Umfragen, Wettbewerben oder Angeboten teilzunehmen, die persönliche Informationen oder finanzielle Transaktionen erfordern.

Vertrauen Sie Ihren Instinkten und bleiben Sie skeptisch: Wenn sich etwas an einer E-Mail seltsam oder verdächtig anfühlt, vertrauen Sie Ihren Instinkten und seien Sie vorsichtig. Es ist besser, skeptisch zu sein und die Echtheit einer E-Mail zu überprüfen, bevor Sie Maßnahmen ergreifen.

Verwenden Sie Sicherheitssoftware und E-Mail-Filter: Installieren Sie renommierte Antivirensoftware und E-Mail-Filter, um Phishing-Versuche zu erkennen und zu blockieren. Diese Tools können dabei helfen, verdächtige E-Mails zu identifizieren und vor bösartigen Inhalten zu schützen.

Leitlinien zur Vermeidung des Anklickens verdächtiger Links oder des Herunterladens von Anhängen aus unbekannten Quellen

Überprüfen der Absenderidentität: Bevor Sie auf Links klicken oder Anhänge herunterladen, überprüfen Sie die Identität des Absenders. Stellen Sie sicher, dass die E-Mail oder Nachricht von einer legitimen Quelle stammt und nicht von einem unbekannten oder verdächtigen Absender.

Überprüfen der E-Mail-Adresse: Untersuchen Sie die E-Mail-Adresse des Absenders sorgfältig. Seien Sie vorsichtig bei E-Mail-Adressen, die falsch geschriebene oder verdächtige Domainnamen verwenden, da sie auf Phishing-Versuche hinweisen können.

Mit dem Mauszeiger über Links fahren, um URLs zu überprüfen: Bewegen Sie den Mauszeiger über Hyperlinks in E-Mails oder Nachrichten (ohne zu klicken), um die Ziel-URL anzuzeigen. Überprüfen Sie, ob die URL mit der offiziellen Website der behaupteten Organisation übereinstimmt. Seien Sie vorsichtig bei verkürzten URLs oder URLs, die zu unbekannten oder verdächtigen Websites weiterleiten.

Vermeiden von unaufgeforderten E-Mails oder Nachrichten: Seien Sie vorsichtig bei unaufgeforderten E-Mails oder Nachrichten von unbekannten Absendern, insbesondere wenn sie Links oder Anhänge enthalten. Löschen oder ignorieren Sie solche E-Mails, um potenzielle Sicherheitsrisiken zu vermeiden.

Achten Sie auf dringende oder verdächtige Anfragen: Seien Sie vorsichtig bei E-Mails oder Nachrichten, die dringende Anfragen oder Drohungen enthalten. Beispiel hierfür sind Warnungen vor Kontosuspendierung, rechtlichen Maßnahmen oder finanzielle Konsequenzen. Betrüger verwenden

oft das Mittel der Dringlichkeit, um Empfänger dazu zu bringen, auf bösartige Links zu klicken oder Anhänge herunterzuladen.

Inhalte mit dem Absender überprüfen: Wenn Sie eine E-Mail oder Nachricht mit Links oder Anhängen von einem bekannten Absender erhalten, aber der Inhalt verdächtig erscheint, überprüfen Sie die Echtheit des Inhalts mit dem Absender über einen separaten Kommunikationskanal (z. B. Telefonanruf oder SMS).

Verwenden von Antivirensoftware und E-Mail-Filtern: Installieren Sie renommierte Antivirensoftware und E-Mail-Filter auf Ihren Geräten, um bösartige Inhalte, einschließlich verdächtiger Links und Anhänge, zu erkennen und zu blockieren. Halten Sie Ihre Antivirensoftware und E-Mail-Filter auf dem neuesten Stand, um die maximale Wirksamkeit zu gewährleisten.

Informieren Sie sich über gängige Phishing-Taktiken: Bleiben Sie über gängige Phishing-Taktiken und -Strategien informiert, die von Cyberkriminellen verwendet werden, um Personen dazu zu bringen, auf bösartige Links zu klicken oder Anhänge herunterzuladen. Informieren Sie sich und Ihre Teammitglieder über die neuesten Phishing-Trends und -Techniken.

Seien Sie vorsichtig in sozialen Medien und Messaging-Apps: Seien Sie vorsichtig beim Klicken auf Links oder Herunterladen von Anhängen aus sozialen Medien, Messaging-Apps oder anderen Online-Plattformen. Betrüger verwenden oft diese Plattformen, um Phishing-Links und Malware zu verbreiten.

Melden Sie verdächtige Aktivitäten: Wenn Sie eine verdächtige E-Mail oder Nachricht mit Links oder Anhängen erhalten, melden Sie diese an die IT-Abteilung Ihrer Organisation oder an die entsprechenden Behörden. Die Meldung verdächtiger Aktivitäten kann dazu beitragen, andere vor Phishing-Betrug zu schützen.

Wichtigkeit der Geheimhaltung persönlicher Informationen auf Social Media Plattformen

Die private Haltung persönlicher Informationen auf sozialen Medien ist aus mehreren Gründen entscheidend:

Schutz vor Identitätsdiebstahl: Persönliche Informationen, die auf sozialen Medien geteilt werden, wie vollständiger Name, Geburtsdatum, Adresse und Kontaktdaten, können von Identitätsdieben ausgenutzt werden, um Ihre Identität zu stehlen. Mit diesen Informationen können Kriminelle betrügerische Konten eröffnen, Kreditkarten beantragen oder andere Formen von Finanzbetrug in Ihrem Namen begehen.

Verhinderung von Cyberstalking und Belästigung: Das Teilen zu vieler persönlicher Informationen auf sozialen Medien kann Sie anfällig für

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

Cyberstalking und Belästigung machen. Böswillige Personen können Ihre persönlichen Informationen verwenden, um Ihren Aufenthaltsort zu verfolgen, Ihre Aktivitäten zu überwachen oder Sie online oder im wirklichen Leben zu belästigen.

Vermeidung von Online-Betrug und Phishing-Angriffen: Cyberkriminelle nutzen häufig auf sozialen Medien geteilte persönliche Informationen, um gezielte Phishing-Angriffe oder Betrug durchzuführen. Sie können Ihre persönlichen Daten verwenden, um überzeugende Nachrichten oder E-Mails zu verfassen, um Sie zur Offenlegung sensibler Informationen oder zum Eingehen auf betrügerische Schemata zu verleiten.

Schutz von Ruf und Privatsphäre: Das Teilen sensibler oder unangemessener Informationen auf sozialen Medien kann Ihren Ruf und Ihre Privatsphäre beeinträchtigen. Arbeitgeber, Kollegen, Familienmitglieder und andere könnten Zugang zu Ihren Social-Media-Profilen haben.

Verhinderung von Social-Engineering-Angriffen: Soziale Medien werden häufig von Cyberkriminellen für Social-Engineering-Angriffe genutzt, bei denen sie Benutzer manipulieren, um vertrauliche Informationen preiszugeben oder Aktionen durchzuführen, die die Sicherheit gefährden. Indem Sie die Menge an persönlichen Informationen, die Sie auf sozialen Medien teilen, begrenzen, reduzieren Sie das Risiko, Opfer von Social-Engineering-Taktiken zu werden.

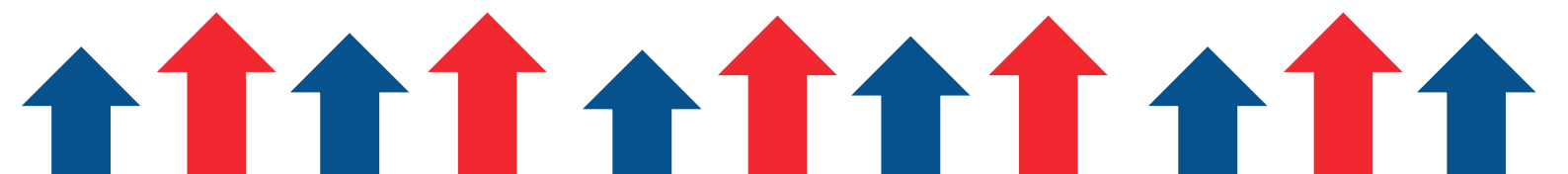
Verbesserte Online-Sicherheit: Das private Halten persönlicher Informationen auf sozialen Medienplattformen trägt zur Verbesserung Ihrer allgemeinen Online-Sicherheit bei. Es verringert die Wahrscheinlichkeit eines unbefugten Zugriffs auf Ihre Konten, minimiert das Risiko von Identitätsdiebstahl und schützt somit Ihre Privatsphäre bzw. wahrt den digitalen Fußabdruck.

Aktivität: Interaktive Sitzung zum Erkennen und Vermeiden verdächtiger Links und Anhänge in simulierten E-Mail-Szenarien.

Das Ziel dieser Aktivität ist es, die TeilnehmerInnen über das Identifizieren und Vermeiden verdächtiger Links und Anhänge in E-Mails durch simulierte Szenarien zu informieren. Die TeilnehmerInnen sollen interaktive Übungen durchführen, indem sie E-Mail-Inhalte analysieren und informierte Entscheidungen zu treffen, ob sie auf Links klicken oder Anhänge herunterladen.

Benötigte Materialien:

1. Simulierte E-Mail-Szenarien
2. Whiteboard oder Flipchart
3. Schreibmaterialien
4. Computer oder mobile Geräte mit Internetzugang (optional)



Einführung (5 Minuten):

1. Begrüßen Sie die TeilnehmerInnen zur interaktiven Sitzung über das Erkennen und Vermeiden verdächtiger Links und Anhänge in E-Mails.
2. Erklären Sie den Zweck der Aktivität: Die Sensibilisierung und das Erlernen von Fähigkeiten der TeilnehmerInnen zur Erkennung von Phishing-Versuchen und zum Schutz vor Cyberbedrohungen.

Präsentation zu Warnhinweisen und bewährten Verfahren (10 Minuten):

1. Geben Sie eine kurze Präsentation zu den Warnhinweisen und bewährten Verfahren zur Identifizierung verdächtiger Links und Anhänge in E-Mails.
2. Diskutieren Sie gemeinsame Merkmale von Phishing-E-Mails, wie generische Grüße, dringende Anfragen, verdächtige URLs und Anfragen nach persönlichen Informationen.
3. Diskutieren Sie bewährte Verfahren zur Vermeidung des Klickens auf Links oder zum Herunterladen von Anhängen aus unbekannten oder verdächtigen Quellen.

Simulierte E-Mail-Szenarien (30 Minuten):

1. Teilen Sie die TeilnehmerInnen in kleine Gruppen auf.
2. Verteilen Sie simulierte E-Mail-Szenarien an jede Gruppe. Jedes Szenario sollte eine E-Mail mit einem Link oder Anhang enthalten, der verdächtig sein könnte.

Beispiel:

Legitime E-Mail von einer Bank:

Subject: Your monthly statement is ready
From: noreply@yourbank.com

Dear Customer,

Your monthly statement is now available in your online banking account. Please log in to your account to view the statement.

Best,
Your Bank

Phishing-E-Mail, die sich als Bank ausgibt:

Subject: Urgent: Account Suspended
From: support@yourbank-security.com

Dear Customer,

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

We have detected unusual activity on your account. Your account has been suspended. Please click the link below to verify your identity and restore your account.

Click here to restore your account.

Best,
Your Bank

In diesem Fall verwendet die E-Mail eine „dringliche“ Wortwahl, um den Empfänger dazu zu drängen, auf den Link zu klicken. Die E-Mail-Adresse des Absenders ist ebenfalls verdächtig und nicht die offizielle E-Mail-Adresse der Bank.

Legitime E-Mail von einem Kollegen:

Subject: Meeting Notes
From: colleague@yourcompany.com

Hi,

Please find the meeting notes attached.

Best,
Colleague

Phishing-E-Mail, die sich als Kollege ausgibt:

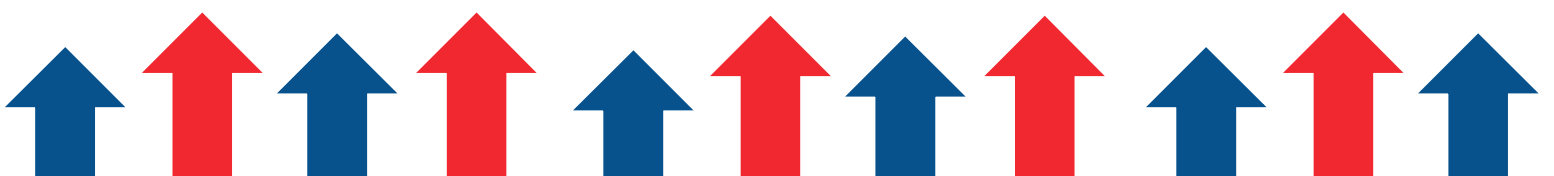
Subject: Urgent: Invoice Due
From: colleage@yourcompany.com

Hi,

The invoice for our vendor is due. Please see the attached invoice and make the payment immediately.

Best,
Colleague

In diesem Fall verwendet die E-Mail eine dringende Sprache und fordert den Empfänger auf, eine Aktion auszuführen, die normalerweise nicht dem gewöhnlichen Vorgehen entspricht. Die E-Mail-Adresse des Absenders enthält auch einen Tippfehler, was ein Anzeichen für einen Phishing-Versuch sein kann.



Weisen Sie die TeilnehmerInnen an, den E-Mail-Inhalt sorgfältig zu analysieren Warnsignale zu identifizieren und darüber zu entscheiden, ob sie auf den Link klicken oder den Anhang herunterladen sollen.

Ermutigen Sie die TeilnehmerInnen, die Beobachtungen und den Entscheidungsprozess innerhalb der Gruppen zu diskutieren.

Gruppendiskussion (15 Minuten):

Versammeln Sie die Gruppe wieder und laden Sie jede Gruppe ein, die Erkenntnisse der simulierten E-Mail-Szenarien zu teilen.

Moderieren Sie eine Diskussion über die von den TeilnehmerInnen identifizierten Warnsignale und die Gründe für die getroffenen Entscheidungen, ob sie auf Links klicken oder Anhänge herunterladen sollen.

Verwenden Sie ein Whiteboard oder Flipchart, um die wichtigsten Erkenntnisse und Einsichten aus der Diskussion festzuhalten.

Reflexion und Erkenntnisse (10 Minuten):

Leiten Sie eine Reflexionssitzung ein, in der die TeilnehmerInnen ihre Gedanken und Erkenntnisse aus der interaktiven Sitzung teilen.

Diskutieren Sie mit den TeilnehmerInnen die Vorkehrungsmaßnahmen, damit man nicht Opfer von Phishing-Versuchen wird und wie man sich vor Cyberbedrohungen im täglichen E-Mail-Verkehr schützen kann.

Fassen Sie die wichtigsten Erkenntnisse zusammen und betonen Sie die Bedeutung von Wachsamkeit und Skepsis im Umgang mit verdächtigen Links und Anhängen in E-Mails.

Abschluss:

Bedanken Sie sich bei den TeilnehmerInnen für ihre aktive Teilnahme an der interaktiven Sitzung.

Ermutigen Sie die TeilnehmerInnen, das erlangte Wissen und die erworbenen Fähigkeiten anzuwenden, um verdächtige Links und Anhänge in ihren E-Mail-Kommunikationen zu identifizieren und zu vermeiden.

Bieten Sie zusätzliche Ressourcen und Unterstützung für TeilnehmerInnen an, die mehr über bewährte Verfahren in der Cybersicherheit erfahren möchten.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

Integration von Fallstudien

Beispiele aus dem wirklichen Leben von Personen, die Opfer von Finanzbetrug wurden

Das Ponzi-Schema von Bernie Madoff:

Eine der berüchtigtsten Finanzbetrug in der Geschichte wurde von Bernie Madoff orchestriert. Madoff führte über mehrere Jahrzehnte hinweg ein Ponzi-Schema, das den Anlegern hohe Renditen versprach. Er lockte Tausende von Anlegern an, darunter Einzelpersonen, Wohltätigkeitsorganisationen und institutionelle Anleger, indem er konsistente und lukrative Renditen versprach. Anstatt jedoch die Gelder wie versprochen anzulegen, verwendete Madoff das Geld neuer Anleger, um Renditen an bestehende Anleger auszuzahlen. Das Schema brach schließlich 2008 zusammen und führte zu Milliardenverlusten für die Anleger. (Hayes, 2023)

Vorschussbetrug:

Der Vorschussbetrug, auch bekannt als **419er-Betrug**, ist ein häufiger Finanzbetrug, der Einzelpersonen über E-Mail oder andere Kommunikationskanäle ins Visier nimmt. Bei einem Vorschussbetrug versprechen Betrüger eine große Geldsumme im Austausch gegen eine geringe Vorauszahlung oder Gebühr. Opfer werden mit Versprechungen von Erbschaften, Lottogewinnen oder Geschäftsmöglichkeiten angelockt, verlieren jedoch letztendlich Geld an die Betrüger. (Grigutytė & Grigutytė, 2023)

Strategien, die angewendet werden können, um nicht Opfer dieser Betrugsmaschen zu werden:

Das Ponzi-Schema von Bernie Madoff:

Sorgfältige Prüfung: Investoren hätten vor der Investition ihres Geldes bei Bernie Madoff eine gründliche Due Diligence durchführen können. Dies würde die Überprüfung der Legitimität der Investmentfirma, die Prüfung von Finanzberichten und die Einholung unabhängiger Drittanbieterprüfungen umfassen.

Frage unrealistische Renditen: Investoren hätten die unrealistischen und konstanten Renditen hinterfragen sollen, die von Madoffs Investmentfirma versprochen wurden. Konstant hohe Renditen bei minimalem Risiko hätten Warnsignale setzen und weitere Untersuchungen auslösen sollen.

E-Mail-Phishing-Betrug:

Identität des Absenders überprüfen: Überprüfen Sie immer die Identität des Absenders, bevor Sie auf E-Mails antworten, die persönliche oder finanzielle Informationen anfordern. Seriöse Organisationen würden niemals sensible Informationen per E-Mail anfordern.

URLs und Links überprüfen: Fahren Sie mit der Maus über Hyperlinks in E-Mails, um die Ziel-URL zu überprüfen, bevor Sie daraufklicken. Seien Sie vorsichtig bei URLs, die nicht mit der offiziellen Website der Organisation übereinstimmen oder verdächtige Domains enthalten.

Kryptowährungsbetrug:

Recherchieren Sie Investitionsmöglichkeiten: Führen Sie gründliche Recherchen durch, bevor Sie in Kryptowährungen investieren oder an Initial Coin Offerings (ICOs) teilnehmen. Überprüfen Sie die Legitimität des Projekts, der Teammitglieder und der Whitepaper, um Investitionen in betrügerische Systeme zu vermeiden.

Vermeiden Sie unrealistische Renditen: Seien Sie skeptisch gegenüber Investitionsmöglichkeiten, die konstant hohe Renditen bei minimalem Risiko versprechen. Kryptowährungsinvestitionen, bergen wie jede andere Investition inhärente Risiken. Garantierte Renditen sollten mit Skepsis betrachtet werden.

Vorschussbetrug:

Seien Sie skeptisch gegenüber unaufgeforderten Angeboten: Seien Sie vorsichtig bei unaufgeforderten E-Mails oder Nachrichten, die große Geldsummen im Austausch für eine geringe Vorauszahlung oder Gebühr versprechen. Üben Sie Vorsicht und hinterfragen Sie die Legitimität solcher Angebote.

Recherchieren und Überprüfen: Recherchieren Sie das Angebot und überprüfen Sie die Identität des Absenders oder der Organisation, bevor Sie antworten. Seriöse Geschäftsmöglichkeiten erfordern in der Regel keine Vorauszahlungen oder Gebühren.

Investitionsbetrug:

Überprüfen Sie Investitionsmöglichkeiten: Führen Sie gründliche Recherchen zu Investitionsmöglichkeiten durch und überprüfen Sie die Legitimität der Investmentfirma oder des Beraters. Überprüfen Sie regulatorische Registrierungen, Lizenzen und Disziplinarhistorien, um die Glaubwürdigkeit sicherzustellen.

Vermeiden Sie Hochdruck-Verkaufstaktiken: Seien Sie vorsichtig bei Investitionsmöglichkeiten, die Hochdruck-Verkaufstaktiken verwenden oder Sie zu schnellen Entscheidungen drängen. Seriöse Investitionsmöglichkeiten lassen Zeit für eine ausführliche Due Diligence und entsprechende Überlegungen.

Aktivität: Gruppenpräsentation zur Analyse von realen Fällen von Finanzbetrug und Vorschlag von Präventivmaßnahmen

Das Ziel dieser Aktivität besteht darin, das Verständnis der TeilnehmerInnen für reale Finanzbetrugsfälle zu vertiefen, die Faktoren zu analysieren, die zu den Betrugsfällen beigetragen haben, und präventive Maßnahmen vorzuschlagen, um sich in Zukunft vor ähnlichen Betrugsfällen zu schützen.

Benötigte Materialien:

1. Liste realer Finanzbetrugsfälle (oben erwähnt)
2. Präsentationsmaterialien (Folien, Handouts usw.)
3. Schreibmaterialien

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

4. Projektor oder Bildschirm (bei Verwendung von Folien)

Anleitung:

Einführung (10 Minuten):

1. Begrüßen Sie die TeilnehmerInnen zur Gruppenpräsentation über die Analyse realer Finanzbetrugsfälle und das Vorschlagen präventiver Maßnahmen.
2. Erläutern Sie den Zweck der Aktivität: die Untersuchung realer Finanzbetrugsfälle, die Identifizierung gemeinsamer Muster und Schwachstellen sowie das Vorschlagen präventiver Maßnahmen zur Risikominderung ähnlicher Betrugsfälle.

Auswahl der Betrugsfälle (10 Minuten):

1. Teilen Sie die TeilnehmerInnen in kleine Gruppen auf.
2. Geben Sie jeder Gruppe eine Liste realer Finanzbetrugsfälle zur Auswahl. Diese Fälle sollten eine Vielzahl von Finanzbetrugsarten abdecken, wie Ponzi-Systeme, Anlagebetrug, Phishing-Betrug, usw.
3. Weisen Sie jede Gruppe an, einen Betrugsfall zur Analyse und Präsentation auszuwählen.

Recherche und Analyse (30 Minuten):

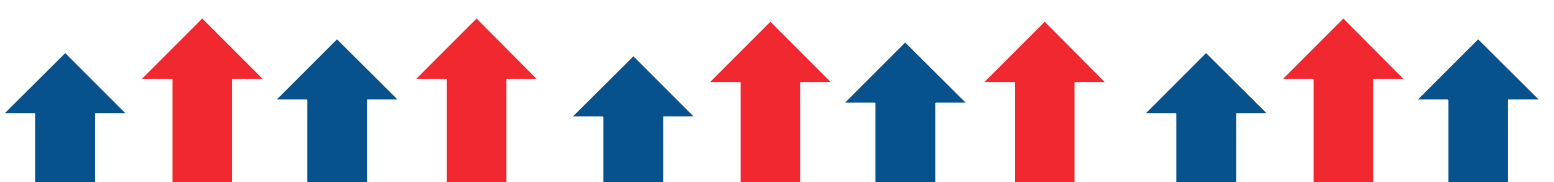
1. Weisen Sie jeder Gruppe Zeit zur Recherche und Analyse des ausgewählten Betrugsfalls zu.
2. Ermutigen Sie die Gruppen, die Details des Betrugsfalls zu untersuchen, einschließlich der Täter, Opfer, verwendeten Methoden, Warnsignale, Auswirkungen und Konsequenzen.
3. Weisen Sie die Gruppen an, gemeinsame Muster, Schwachstellen und Faktoren zu identifizieren, die zum Erfolg des Betrugs beigetragen haben.

Präventivmaßnahmen (30 Minuten):

1. Nach Analyse des Betrugsfalls sollten die Gruppen präventive Maßnahmen zum Schutz vor ähnlichen Betrugsfällen in Zukunft brainstormen und vorschlagen.
2. Ermutigen Sie die Gruppen, eine Reihe von präventiven Maßnahmen in Betracht zu ziehen, darunter regulatorische Reformen, Verbraucherbildung, Aufklärungskampagnen, technologische Lösungen und Durchsetzungsmaßnahmen.
3. Jede Gruppe sollte eine Liste präventiver Maßnahmen erstellen und diese basierend auf ihrer Wirksamkeit und Durchführbarkeit priorisieren.

Gruppenpräsentationen (40 Minuten):

1. Weisen Sie jeder Gruppe Zeit zur Präsentation ihrer Analyse des Betrugsfalls und zur Vorstellung präventiver Maßnahmen zu.
2. Ermutigen Sie die Gruppen, Präsentationsmaterialien (Folien, Handouts usw.) zur Unterstützung ihrer Präsentationen zu verwenden.
3. Nach jeder Präsentation leiten Sie eine kurze Fragerunde ein, um anderen Teilnehmern die Möglichkeit zu geben, Fragen zu stellen und Feedback zu geben.



Diskussion und Reflexion (20 Minuten):

1. Schließen Sie die Gruppenpräsentationen mit einer Diskussions- und Reflexionssitzung ab.
2. Ermutigen Sie die TeilnehmerInnen, gemeinsame Themen, Einsichten und Lektionen aus den Betrugsfällen und vorgeschlagenen präventiven Maßnahmen zu diskutieren.
3. Leiten Sie eine Diskussion über die Bedeutung proaktiver Maßnahmen zur Verhinderung von Finanzbetrug und zum Schutz von Verbrauchern und Anlegern.

Abschluss (10 Minuten):

1. Bedanken Sie sich bei den TeilnehmerInnen für ihre Teilnahme und ihre Beiträge zu den Gruppenpräsentationen.
2. Fassen Sie die wichtigsten Erkenntnisse und Einsichten aus der Aktivität zusammen.
3. Betonen Sie die Bedeutung kontinuierlicher Wachsamkeit, Verbraucherbildung und regulatorischer Bemühungen im Kampf gegen Finanzbetrug.

Übung

Selbstgesteuertes Lernen

Schlagen Sie den TeilnehmerInnen vor, mehr über die Themen zu erfahren, und empfehlen Sie einige zusätzliche Lektüren wie:

Identitätsdiebstahl, betrügerische Transaktionen und Cybersicherheitsbedrohungen:

1. Identity Theft Resource Centre (https://www.idtheftcenter.org/) - Bietet Informationen, Ressourcen und Unterstützung für Opfer von Identitätsdiebstahl.
2. Federal Trade Commission (FTC) Identity Theft Website (https://www.identitytheft.gov/) - Bietet eine schrittweise Anleitung zur Prävention, Erkennung und Wiederherstellung von Identitätsdiebstahl.

Bedeutung von Sicherheitsmaßnahmen und grundlegenden Sicherheitsmaßnahmen:

1. StaySafeOnline.org (https://staysafeonline.org/) - Bietet Ressourcen und Tipps für Online-Sicherheit und Cyber-Sicherheitsbewusstsein.
2. Cybersecurity & Infrastructure Security Agency (CISA) (https://www.cisa.gov/) - Bietet Cyber-Sicherheitsressourcen, Tipps und bewährte Verfahren für Einzelpersonen und Organisationen.

Erkennen des Betrugs und Cybersicherheitsbewusstsein:

1. FBI Internet Crime Complaint Centre (IC3) (https://www.ic3.gov/) - Ermöglicht Benutzern die Meldung von Internetkriminalität und bietet Ressourcen zur Prävention von Cyberkriminalität.
2. Better Business Bureau (BBB) Scam Alerts (https://www.bbb.org/scamtracker) - Bietet Betrugswarnungen, Tipps und Ressourcen für Verbraucher und Unternehmen.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

Fallstudien zu realen Betrugsfällen und Strategien zur Vermeidung:

1. Securities and Exchange Commission (SEC) (https://www.sec.gov/) - Bietet Ressourcen und Informationen zur Anlegererziehung, Warnungen und Durchsetzungsmaßnahmen.
2. Consumer Financial Protection Bureau (CFPB) (https://www.consumerfinance.gov/) - Bietet Ressourcen und Tools für Verbraucher, einschließlich Betrugswarnungen und Berichten über Finanzbetrug.

Quiz-Bewertung

Quiz: Identifizierung häufiger Sicherheitsrisiken und Erkennen von Betrugsmustern

Anweisungen:

1. Lesen Sie jede Frage sorgfältig durch und wählen Sie die beste Antwort aus.
2. Wählen Sie jene Option aus, die die richtige Antwort am besten repräsentiert.
3. Am Ende des Quiz zählen Sie Ihre Punktzahl zusammen, um zu sehen, wie gut Sie abgeschnitten haben.

Was ist Identitätsdiebstahl?

a) Eine Art von Malware, die den Computer infiziert und persönliche Informationen stiehlt.
b) Die unbefugte Verwendung der persönlichen Informationen einer anderen Person, um Betrug oder andere Verbrechen zu begehen.
c) Ein Finanzbetrug, der betrügerische Anlagepläne beinhaltet.
d) Eine Cyberbedrohung, die auf Online-Bankkonten abzielt.

Welche der folgenden Eigenschaften kennzeichnet Phishing-E-Mails?

a) Personalisierte Grüße, die den Empfänger mit Namen ansprechen.
b) Anfragen nach sensiblen Informationen wie Passwörtern oder Kreditkartennummern.
c) Legitime Absender-E-Mail-Adressen, die mit der offiziellen Domain der Organisation übereinstimmen.
d) Offizielle Logos und Marken von vertrauenswürdigen Organisationen.

Was ist ein Ponzi-Schema?

a) Eine Art von Phishing-Angriff, der Einzelpersonen über betrügerische E-Mails angreift.
b) Ein Anlagebetrug, der Anlegern hohe Renditen bei minimalem Risiko verspricht.
c) Eine Cyberbedrohung, die Schwachstellen in Software oder Systemen ausnutzt.
d) Eine Art von Malware, die entwickelt wurde, um persönliche Informationen von Computern zu stehlen.

Was ist der Zweck der Zwei-Faktor-Authentifizierung?

a) Online-Konten durch die Anforderung mehrerer Formen der Verifizierung zu sichern.
b) Phishing-Angriffe durch Verschlüsselung von E-Mail-Kommunikationen zu verhindern.
c) Sich vor Identitätsdiebstahl zu schützen, indem man Kreditberichte überwacht.
d) Malware von infizierten Geräten zu erkennen und zu entfernen.

Welches der folgenden ist ein Warnzeichen für einen möglichen Betrug?

a) Dringende Anfragen nach persönlichen Informationen oder sofortigem Handeln.
b) Personalisierte E-Mails, die den Empfänger mit Namen ansprechen.
c) Offizielle Logos und Marken von seriösen Organisationen.
d) Anfragen nach Feedback oder Umfragen von vertrauenswürdigen Quellen.

Was ist die wichtigste Bedeutung regelmäßiger Software-Updates und Gerätewartung?

a) Sicherheitsrisiken und Malware-Infektionen zu verhindern.
b) Online-Konten mit starken Passwörtern zu sichern.
c) Identitätsdiebstahl und Finanzbetrug zu verhindern.
d) Sicherheitsanfälligkeiten zu mindern und vor Cyberbedrohungen zu schützen.

Welches der folgenden ist KEINE häufige Eigenschaft von legitimen Anlagechancen?

a) Garantierte hohe Renditen bei minimalem Risiko.
b) Angemessene regulatorische Registrierung und Überwachung.
c) Transparente Dokumentation, die Anlageinformationen und -risiken umreißt.
d) Erhöhter Druck, eine schnelle Anlageentscheidungen, ohne vorgelagerter Due Diligence zu treffen.

Was ist die Bedeutung, persönliche Informationen auf Social-Media-Plattformen privat zu halten?

a) Sich vor Identitätsdiebstahl und Cyberstalking zu schützen.
b) Phishing-Angriffe und Malware-Infektionen zu verhindern.
c) Online-Konten mit Zwei-Faktor-Authentifizierung zu sichern.
d) Software-Schwachstellen und Gerätewartungsprobleme zu vermeiden.

Antworten:

b) Die unbefugte Verwendung der persönlichen Informationen einer anderen Person, um Betrug oder andere Verbrechen zu begehen.

b) Anfragen nach sensiblen Informationen wie Passwörtern oder Kreditkartennummern.

b) Ein Anlagebetrug, der Anlegern hohe Renditen bei minimalem Risiko verspricht.

a) Online-Konten durch die Anforderung mehrerer Formen der Verifizierung zu sichern.

a) Dringende Anfragen nach persönlichen Informationen oder sofortigem Handeln.

d) Sicherheitsanfälligkeiten zu mindern und vor Cyberbedrohungen zu schützen.

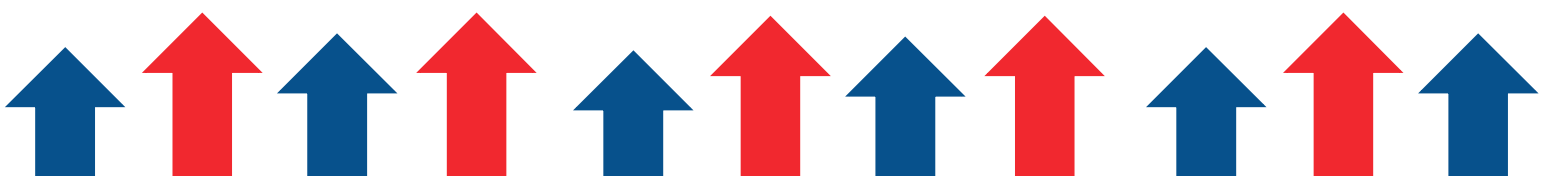
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

a) Garantierte hohe Renditen bei minimalem Risiko.

a) Sich vor Identitätsdiebstahl und Cyberstalking zu schützen.

Bewertung:

- **8 richtige Antworten**: Ausgezeichnet! Sie haben ein hervorragendes Verständnis für häufige Sicherheitsrisiken und Betrugsmuster.
- **5-7 richtige Antworten**: Gut gemacht! Sie haben ein gutes Verständnis der Konzepte, könnten aber von einer weiteren Überprüfung profitieren.
- **4 oder weniger richtige Antworten**: Überlegen Sie, das Material noch einmal zu überprüfen, um Ihr Verständnis für häufige Sicherheitsrisiken und Betrugsmuster zu verbessern.



ONLINE SICHER EINKAUFEN

Einführung in das Online-Shopping

Das Hauptziel dieses Unterkapitels ist es, den TeilnehmerInnen die Merkmale und Vorteile des Online-Shoppings näherzubringen. Online einzukaufen, bietet eine bequeme Möglichkeit, von zuhause aus einzukaufen. In diesem Unterthema werden die TeilnehmerInnen verschiedene Aspekte der Online-Shopping-Websites erkunden und die notwendigen Schritte zum Kauf eines Artikels durchführen - ohne den Kauf tatsächlich abzuschließen. Das Ziel ist es, eine praktische Erfahrung zu ermöglichen, um den Prozess und die Funktionen eines Online-Einkaufs zu verstehen, ohne den endgültigen Kauf zu tätigen.

Durchstöbern von Online-Shops

Das Ziel liegt darin, das Verständnis der TeilnehmerInnen für das Online-Shopping zu vertiefen, indem der Schwerpunkt auf dem „Durchstöbern" der Online-Shops liegt, ohne dass ein Kauf notwendig ist. Es soll den TeilnehmerInnen verdeutlicht werden, dass man Online-Shops erkunden, Artikel ansehen und durch verschiedene Kategorien navigieren kann, ohne sich zum Kauf zu verpflichten. Dies ermöglicht es den TeilnehmerInnen, sich mit dem Layout und den Funktionen verschiedener Online-Shops vertraut zu machen, zu verstehen, wie Produkte präsentiert werden und wie der Einkaufsprozess strukturiert ist.

Durch einfaches Durchstöbern können die Lernenden die Benutzeroberfläche, die Suchfunktionen und die allgemeine Erfahrung des Online-Shoppings kennenlernen, ohne den Druck eines Kaufs zu verspüren. Diese praktische Erkundung ist entscheidend, um ihr Vertrauen und Verständnis für die Online-Shopping-Umgebung zu stärken.

Aktivität 1 – Einen Online-Shop durchstöbern

Die Ziele dieser Aktivität umfassen das Bereitstellen einer praktischen Erfahrung für die TeilnehmerInnen, um in einer Online-Shopping-Plattform zu navigieren und die wesentlichen Schritte eines Kaufs zu verstehen. Die Aktivität sollte damit beginnen, dass die Lernenden angewiesen werden, das Internet zu nutzen und eine spezifische Website wie Amazon besuchen. Durch das Erkunden der Startseite und das Erlernen der Nutzung von Funktionen wie der Suchleiste, den Abteilungstabs und der Navigation durch Kategorien wie „Geschenke" und „Bücher" werden die Lernenden mit dem Layout und den Funktionen der Website vertraut gemacht.

Ziel dieser Aktivität ist es, den Prozess der Verfeinerung von Suchanfragen mithilfe von Filteroptionen und das Navigieren zwischen den Seiten zu veranschaulichen. Der Hauptfokus liegt darauf, das schrittweise Verfahren eines Online-Kaufs zu erklären, von der Suche nach dem Artikel über das Hinzufügen zum Warenkorb, das Sammeln der Produkte bis zur Kasse, das Eingeben der Lieferdetails bis hin zur endgültigen Bezahlung. Diese schrittweise Anleitung soll den TeilnehmerInnen den Ablauf eines Online-Kaufs verständlich machen und ihnen die einzelnen Schritte näherbringen, die auch bei einem physischen Einkauf erforderlich sind.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

Schritt-für-Schritt-Anleitung

1. Bitten Sie Ihren Lernenden, das Internet zu öffnen.
2. Bitten Sie Ihren Lernenden, www.amazon.es (oder eine andere Länderseite) zu besuchen.
3. Erklären Sie die Amazon-Startseite:

- Suchleiste.
- Abteilungstabs.

4. Erkunden Sie die Startseite.
5. Bitten Sie die TeilnehmerInnen, auf den Geschenke-Tab zu klicken und unter der Kategorie Geschenke „Bücher“ auszuwählen.
6. Erkunden Sie die Ergebnisseite der Bücher.
7. Erklären Sie, dass Sie die Filteroptionen auf der linken Seite verwenden können, um Ihre Suche zu verfeinern.
8. Klicken Sie auf die Zurück-Schaltfläche des Browsers, um zur Startseite zurückzukehren.

Einen Artikel online erwerben

Das Ziel dieses Unterthemas ist es, die Lernenden mit den wesentlichen Schritten des Online-Einkaufs vertraut zu machen. Die Erklärung beginnt damit, den digitalen Kaufprozess mit dem eines physischen Geschäfts zu vergleichen und die Schritte in eine einfache Abfolge zu unterteilen. Zunächst werden die TeilnehmerInnen in die grundlegenden Schritte eingeführt, die darin bestehen, den gewünschten Artikel im Online-Shop zu finden, ihn in den virtuellen Warenkorb zu legen, zur Kasse zu gehen, die erforderlichen Lieferdetails einzugeben und die Transaktion durch die Zahlung abzuschließen. Indem der Online-Kaufprozess auf diese Weise dargestellt wird, soll er vereinfacht und entmystifiziert werden, sodass die Lernenden die Schritte leichter verstehen und sich im Online-Einkauf zurechtfinden können, ähnlich wie bei ihren gewohnten Einkäufen im Geschäft. Dieser strukturierte Ansatz soll das Vertrauen und das Verständnis der Lernenden stärken und sie befähigen, effektiv und sicher an Online-Transaktionen teilzunehmen.

Aktivität 2 – Ein E-Book Kindle Online kaufen

Das Hauptziel dieser Aktivität ist es, die TeilnehmerInnen durch die Schritte eines Online-Kaufs zu leiten und dabei entscheidende Faktoren für ein sicheres und seriöses Online-Einkaufserlebnis hervorzuheben. Die TeilnehmerInnen sollten auf eine bestimmte Website wie Amazon geleitet werden, wo sie die Startseite erkunden und deren Authentizität kritisch beurteilen können. Wichtige Überlegungen sind dabei die Überprüfung der Anzeige einer Postadresse, Telefonnummer und einer sichtbaren Rückgabepolitik auf der Website.

Der Schritt-für-Schritt-Kaufprozess wird in einem Selbstversuch erkundet, wobei der Trainer jede Phase erklärt und dabei wichtige Sicherheitsmaßnahmen hervorhebt, wie z. B. die Webadresse, die mit „https“ beginnt und somit eine sichere Transaktion anzeigt. Die Lernenden sollten daran erinnert werden, dass sie keinen tatsächlichen Kauf tätigen, aber wenn sie es täten, würden sie Zahlungsdetails eingeben und eine Bestätigung erhalten. Darüber hinaus wird in der Aktivität auch die Erklärung von Zahlungsoptionen wie Kreditkarte und PayPal behandelt.

Nach der Übung sollten die Lernenden ermutigt werden, die Zurück-Taste des Browsers zu verwenden, um zur Startseite zurückzukehren, wobei sie darauf hingewiesen werden, dass dabei alle eingegebenen Informationen auf der Website gelöscht werden. Dies unterstreicht die Bedeutung der Online-Sicherheit und des Datenschutzes. Diese umfassende Übung zielt darauf ab, die Lernenden darüber aufzuklären, wie man die Anzeichen einer seriösen Website erkennt, den sicheren Zahlungsprozess versteht und sichere Surfgewohnheiten während des Online-Einkaufs entwickelt.

Schritt-für-Schritt-Anleitung

Erklären Sie den TeilnehmerInnen, dass sie eine Schopping-Website besuchen und die Schritte zum Online-Kauf eines Artikels durchlaufen werden, aber nichts tatsächlich einkaufen werden.

1. Bitten Sie Ihren Lernenden, www.amazon.es (oder eine andere Länderseite) zu besuchen.

2. Erkunden Sie die Startseite – **WICHTIG**:

- **Ist die Seite echt?**

- **Wird eine Postadresse und Telefonnummer angezeigt?**

- **Haben sie eine Rückgabepolitik?**

1. Bitten Sie Ihren Lernenden, die Schritte des Kaufprozesses zu folgen.

2. Erklären Sie jeden Schritt, während Sie vorgehen.

3. Wenn sie die Zahlungsseite der Website erreichen, bitten Sie Ihren Lernenden, die Webadresse anzusehen – sie sollte mit https beginnen – **WICHTIG**: Überprüfen Sie, dass die Webadresse im Browser mit https (statt http) beginnt – dies bedeutet, dass eine Art Sicherheit beim Umgang mit Ihrem Geld verwendet wird.

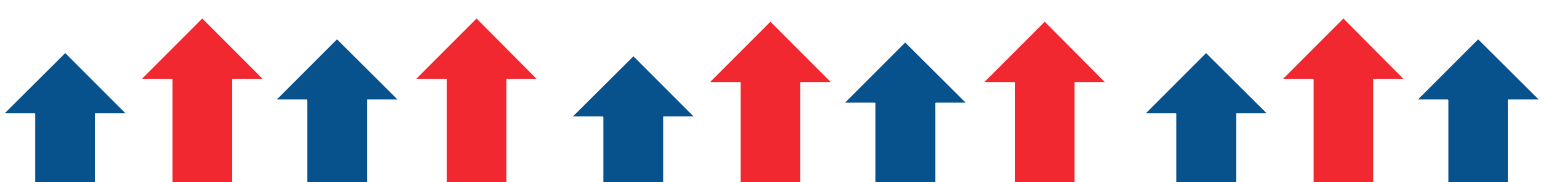
4. Erklären Sie den TeilnehmerInnen, dass er, wenn er den Artikel kaufen würde, nun seine Zahlungsdetails eingeben und eine Bestätigung seines Kaufs erhalten würde. (nicht tatsächlich durchführen!)

5. Erklären Sie die Zahlungsoptionen:

   Kreditkarte; PayPal

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

6.	Wenn die Übung abgeschlossen ist, bitten Sie die TeilnehmerInnen, die Zurück-Schaltfläche des Browsers zu verwenden, um zur Startseite zurückzukehren. **Hinweis**: Die Verwendung der Zurück-Schaltfläche des Browsers löscht alle Informationen, die Sie auf der Website eingegeben haben.



Online-Romantik-Betrug

Online-Romantik-Betrug ist eine unehrliche und raffinierte Art von Cyberkriminalität, bei der Betrüger die emotionalen Bindungen von Opfern ausnutzen, um sie ihres Geldes zu berauben. Um das Vertrauen und die Nähe gutgläubiger Opfer zu gewinnen, übernehmen Betrüger häufig falsche Identitäten und scheinen romantisch an ihnen interessiert zu sein. Diese Kriminellen verwenden kreative Strategien, wie das Erfinden fesselnder Geschichten und das Darstellen als perfekte Partner, um Opfer in dem Glauben zu wiegen, sie seien sicher.

Sobald Vertrauen aufgebaut wurde, kann der Betrüger die Gefühle des Opfers ausnutzen, um sie dazu zu bringen, Geld zu senden oder sensible finanzielle oder persönliche Daten preiszugeben. Übermäßig dramatische oder makellose Lebensgeschichten, eine Unwilligkeit, sich persönlich zu treffen, überhastete Liebes- oder Hingabeerklärungen und Forderungen nach finanzieller Unterstützung sind Warnsignale für Online-Romantik-Betrug. Um die Wahrscheinlichkeit zu verringern, Opfer dieser betrügerischen Machenschaften zu werden, ist es entscheidend, Vorsicht, Skepsis und Wachsamkeit bei der Teilnahme an Online-Interaktionen walten zu lassen. Online-Romantik-Betrug nährt sich von den Emotionen und dem Vertrauen der Menschen.

Aktivität 3 – Online-Romantik-Betrug erkennen

Die Aktivität zielt darauf ab, die Teilnehmer über die Identifizierung von Warnzeichen potenziellen Online-Romantik-Betrugs aufzuklären. Es legt den Schwerpunkt darauf, Warnsignale wie eine übermäßig perfekte Persönlichkeit, das Vermeiden von persönlichen Treffen, schnelle Liebesbekundungen und die Bitte um finanzielle Unterstützung zu erkennen. Darüber hinaus bietet es prägnante Sicherheitsratschläge, die dafür plädieren, Online-Hintergrundüberprüfungen durchzuführen, persönliche Informationen zurückzuhalten und dem eigenen Bauchgefühl zu vertrauen, wenn man sich in einer Beziehung unwohl fühlt.

Die Aktivität ermutigt zu offenen Diskussionen, die es den TeilnehmerInnen ermöglicht, Fragen zu stellen und zu beantworten, während sie Meinungen, Bedenken und persönliche oder beobachtete Erfahrungen mit Online-Romantik-Betrug teilen. Dieser interaktive Austausch fördert das Bewusstsein und die Vorbereitung gegen potenziell betrügerische Aktivitäten beim Online-Dating und ermöglicht es Einzelpersonen, diese Beziehungen vorsichtiger und vernünftiger zu bewerten.

Schritt-für-Schritt-Anleitung

Diskutieren Sie einige typische Warnsignale, die auf einen Online-Romantik-Betrug hinweisen könnten. Diese könnten sein:

- Zu perfekt, um wahr zu sein: Seien Sie vorsichtig, wenn die Person übermäßig perfekt erscheint oder ihre Lebensgeschichte übermäßig dramatisch klingt.
- Vermeidung persönlicher Treffen: Es ist ein Warnzeichen, wenn die andere Person ständig Ausreden macht, um persönliche Treffen zu vermeiden.
- Schnelle Liebesbekundungen: Es könnte ein Hinweis sein, wenn sie ihre Liebe oder Hingabe extrem früh in der Beziehung zeigen.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

- Geldforderungen: Geben Sie niemals Bargeld oder finanzielle Details an einen Fremden weiter, den Sie nicht persönlich getroffen haben.

1. Geben Sie einige kurze Sicherheitsratschläge:

- Führen Sie immer eine Online-Hintergrundüberprüfung einer Person durch, um nach Unstimmigkeiten zu suchen.

- Geben Sie keine persönlichen Informationen preis: Behalten Sie Ihre Hausadresse, Bankinformationen und Sozialversicherungsnummer für sich.

- Wenn etwas seltsam erscheint, vertrauen Sie Ihrem Bauchgefühl! Hören Sie auf Ihr Bauchgefühl.

2. Geben Sie jedem die Möglichkeit, Fragen zu stellen und zu beantworten.

- Ermutigen Sie die TeilnehmerInnen, ihre Meinungen, Bedenken und persönlichen oder beobachteten Erfahrungen mit Online-Romantik-Betrug zu diskutieren.

Aktivität 4 – Ein Video über sicheres Einkaufen

Das Ziel dieser Aktivität ist es, die Lernenden dabei zu unterstützen, Sicherheitsmaßnahmen beim Online-Shopping zu erkennen und umzusetzen. Die Aktivität sollte damit beginnen, dass die TeilnehmerInnen aufgefordert werden, www.getsafeonline.org zu besuchen, und dann in den Bereich "Videos ansehen" zu navigieren, um das Video "Online-Shopping" auszuwählen. Nach Abschluss des Videos sollten die Lernenden angewiesen werden, zu www.easons.com zu gehen und die Website kritisch zu bewerten, indem sie bestimmte Fragen beantworten: Ob die Website eine Datenschutzrichtlinie anzeigt und ob sie eine Kontaktadresse angibt.

Diese Aktivität zielt darauf ab, die TeilnehmerInnen dazu zu ermutigen, sich mit Bildungsmaterialien zur Online-Sicherheit auseinanderzusetzen, und dann ihr Wissen praktisch anzuwenden, indem sie die Sicherheitsmaßnahmen und die Transparenz einer tatsächlichen Einkaufswebsite bewerten. Durch die Kombination theoretischer Einblicke aus dem Video mit einer praktischen Website-Bewertung können die Lernenden aktiv wesentliche Sicherheitsvorkehrungen beim Online-Shopping erkennen und identifizieren. Dieser Prozess ermöglicht ein praktisches Lernerlebnis und unterstreicht die Bedeutung von Datenschutzrichtlinien und Kontaktinformationen für ein sicheres Online-Shopping-Erlebnis.

ALTERNATIVE ZAHLUNGSMÖGLICHKEITEN

Einführung in alternative Zahlungsmethoden

Konventionelle Zahlungsmethoden wie Bargeld und Kreditkarten können unter bestimmten Bedingungen und Konstellationen der Gesellschaft und der Umwelt nicht den bestmöglichen Nutzen bieten. Dieses Unterthema adressiert dies, indem es alternative Zahlungsmethoden vorgestellt werden:

- **Digitale Geldbörsen**: Durch Vereinfachung von Online-Transaktionen und Beseitigung der Notwendigkeit von Bargeld und Papierrechnungen fördern diese elektronischen Karten ein papierloses Finanzsystem.
- **Mobile Zahlungen**: Für eine Vielzahl von Dienstleistungen und Gütern übernehmen diese auf mobilen Geräten ausgeführten Dienste die Rolle herkömmlicher Zahlungsmethoden wie Bargeld oder Karten.
- **Kryptowährungen**: Mithilfe der Blockchain-Technologie ermöglichen dezentralisierte und sichere digitale Währungen Transaktionen ohne die Notwendigkeit von Zentralbanken. Die verringert möglicherweise die Abhängigkeit von etablierten Finanzinstituten.

Alternative Zahlungsmethoden beziehen sich auf nicht traditionelle Arten der Durchführung finanzieller Transaktionen jenseits von Bargeld bzw. Kredit-/Debitkarten. Diese Methoden haben aufgrund ihrer Bequemlichkeit, Zugänglichkeit und oft ihrer Integration in digitale Plattformen an Popularität gewonnen. Prepaid-Karten, Banküberweisungen, digitale Geldbörsen, Kryptowährungen, Treueprogramme, lokale Karten und gestaffelte Zahlungsoptionen sind nur einige der Möglichkeiten, die in diese Kategorie fallen. Aufgrund ihrer Benutzerfreundlichkeit und Sicherheit wurde ihre Akzeptanz durch die Epidemie noch weiter beschleunigt.

- **Auswirkungen auf die Umwelt und die Gesellschaft**: Die Verwendung alternativer Zahlungsmethoden für digitale Transaktionen hat diverse Vorteile.
- **Ökologische Vorteile**: Digitale Transaktionen zeichnen sich durch einen geringeren Papierverbrauch, einen kleineren CO2-Fußabdruck und eine bessere Energieeffizienz aus. Sie verringern die Schäden, die die Produktion und den Transport von physischem Geld erfordert.
- **Die Auswirkungen von Kryptowährungen auf die Gesellschaft** zeigen sich in ihrer Fähigkeit, Transaktionskosten drastisch zu senken, Transaktionen zu beschleunigen und die finanzielle Inklusion (insbesondere in marginalisierten Gemeinschaften) zu fördern. Dies hilft, lokale Wirtschaften zu unterstützen und finanzielle Dienstleistungen für Menschen bereitzustellen, die keinen Zugang zu traditionellen Institutionen haben.

Aufgrund mehrerer Überlegungen bieten digitale Transaktionen eine ökologischere Option als traditionelle Währungstransaktionen, die ihrerseits erhebliche Umweltauswirkungen haben.

- **Verringerte Umweltauswirkungen**: Die Herstellung, Verteilung und der Druck physischer Währung hinterlassen alle eine erhebliche Papierbilanz, die zum Baumverlust beiträgt. Die weit verbreitete Verwendung von Bargeld hat negative Umweltauswirkungen wie die Entwaldung und die Zunahme von Treibhausgasemissionen. Darüber hinaus führt das Tragen von Bargeld zu

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

Banken und Geldautomaten zu einem erhöhten Kraftstoffverbrauch und Emissionen durch den Transport von Autos.
- **Energieeffizienz digitaler Transaktionen**: Elektronisch durchgeführte digitale Transaktionen erfordern andererseits weniger Energie und erhebliche physische Ausrüstung. Um ihre Gesamtwirkung auf die Umwelt zu verringern, werden die meisten digitalen Transaktionen in Rechenzentren abgewickelt, die mit erneuerbaren Energien betrieben werden. Diese Einrichtungen sind darauf ausgelegt, so energieeffizient wie möglich zu sein und senken dadurch erheblich ihren CO2-Fußabdruck.

Es gibt mehrere potenzielle Vorteile von Kryptowährungen, insbesondere für benachteiligte Bevölkerungsgruppen, die nach Finanzdienstleistungen suchen:

- **Geringere Transaktionskosten**: Banken und Überweisungsunternehmen erheben häufig hohe Gebühren für traditionelle internationale Geldüberweisungen. Diese Kosten werden durch Kryptowährungen erheblich reduziert, was internationale Geldtransfers vernünftiger und möglich macht.
- **Schnellere Transaktionen**: Kryptowährungstransaktionen sind im Vergleich zu herkömmlichen Bankensystemen für ihre Schnelligkeit bekannt. Diese Geschwindigkeit ist besonders wichtig für Menschen, die auf rechtzeitige Überweisungen angewiesen sind, um tägliche Kosten oder unvorhergesehene Notfälle zu decken.
- **Finanzielle Inklusion und lokale Wirtschaften**: Durch die Bereitstellung von Finanzdienstleistungen für Menschen ohne Zugang zu traditionellen Bankinstitutionen können Kryptowährungen finanzielle Lücken in abgelegenen oder verarmten Gebieten schließen. Diese allumfassende Strategie kann die regionale Wirtschaft erheblich ankurbeln und benachteiligten Menschen mehr Einfluss geben.

Arten von alternativen Zahlungsmitteln

Alternative Zahlungsmethoden beziehen sich auf verschiedene nicht-traditionelle Finanztransaktionsmethoden. Einige Beispiele für alternative Zahlungsmethoden sind:

- **Prepaid-Karten**: Dies sind Karten, die mit einem bestimmten Geldbetrag vorab geladen sind und verwendet werden können, um Einkäufe zu tätigen, bis das Guthaben aufgebraucht ist.
- **Banküberweisungen**: Diese Methode ermöglicht es VerbraucherInnen, Waren und Dienstleistungen online über direkte Online-Überweisungen von ihrem Bankkonto zu bezahlen.
- **Digitale Geldbörsen**: Dies sind Software- oder Hardwarelösungen, mit denen Benutzer elektronische Zahlungen tätigen können. Sie können verwendet werden, um mehrere Zahlungsmethoden wie Kreditkarten und Bankkonten zu speichern und Einkäufe online oder in Geschäften zu tätigen.
- **Kryptowährungen**: Dies sind digitale oder virtuelle Währungen, die Kryptographie zur Sicherheit verwenden und unabhängig von einer Zentralbank operieren. Sie können verwendet werden, um Einkäufe online oder in Geschäften zu tätigen, die sie als Zahlungsmittel akzeptieren.
- **Treueprogramme**: Diese Programme ermöglichen es Verbrauchern, Punkte oder Belohnungen für Einkäufe bei einem bestimmten Händler oder einer bestimmten Marke zu sammeln. Die Punkte oder Belohnungen können dann für Rabatte oder kostenlose Produkte eingelöst werden.

- **Lokale Karten**: Dies sind Kredit- oder Debitkarten, die von lokalen Banken oder Finanzinstituten ausgegeben werden und nur innerhalb eines bestimmten Landes oder einer Region verwendet werden können.
- **Verzögerte Zahlung und Ratenzahlungsoptionen**: Diese Optionen ermöglichen es Verbrauchern, die Zahlung für einen Kauf zu verzögern oder ihn in Raten über einen bestimmten Zeitraum zu bezahlen.

Aktivität 1: Verschiedene Arten von alternativen Zahlungsmitteln

Das Hauptziel dieser Aktivität besteht darin, den TeilnehmerInnen ein Handout zur Verfügung zu stellen, die eine Vielzahl verschiedener Zahlungsoptionen darstellt und erläutert. Für jede Methode wird eine kurze Beschreibung bereitgestellt, die Prepaid-Karten, Banküberweisungen, digitale Geldbörsen, Kryptowährungen, Treueprogramme, lokale Karten und verzögerte Zahlungsoptionen umfasst. Das Ziel ist es, den TeilnehmerInnen ein grundlegendes Verständnis für verschiedene Zahlungsmethoden zu vermitteln, wobei die zahlreichen Vorteile, Funktionen und Situationen hervorgehoben werden, in denen jede Methode nützlich sein könnte. Am Ende der Aktivität sollten die TeilnehmerInnen ein grundlegendes Verständnis für alternative Zahlungsoptionen haben und in der Lage sein, die möglichen Verwendungen und Vorteile jeder Methode in verschiedenen finanziellen Situationen zu bewerten.

Schritt-für-Schritt-Anleitung

1. Verteilen Sie das Handout an die TeilnehmerInnen.

2. Fragen Sie die TeilnehmerInnen, ob sie bereits eine dieser Zahlungsmethoden verwendet haben und falls ja, wie ihre Erfahrungen damit waren.

Aktivität 2: Vorteile und Nachteile

Die Ziele dieser Aktivität bestehen darin, kritisches Denken zu fördern und die TeilnehmerInnen zur aktiven Teilnahme an der Abwägung der Vor- und Nachteile verschiedener Zahlungsoptionen zu ermutigen. Auf der Tafel oder dem Flipchart wird ein organisiertes Feld erstellt, das die Teilnahme an einem Gruppengespräch fördert. Das Ziel der Übung besteht darin, die Vor- und Nachteile verschiedener alternativer Zahlungsoptionen zu untersuchen und zu verstehen.

Durch diese Übung können die Lernenden die Vorteile dieser Strategien identifizieren, darunter mehr Flexibilität, eine breitere Kundenbasis und mögliche Kosteneinsparungen für Unternehmen. Gleichzeitig denken sie über mögliche Nachteile nach, wie etwa die begrenzte Akzeptanz durch Unternehmen, die Notwendigkeit mehrerer Zahlungsoptionen und die unterschiedlichen Grade des Betrugsschutzes, den verschiedene Alternativen bieten. Die TeilnehmerInnen gewinnen durch diesen Vergleich ein Verständnis für die Komplexität alternativer Zahlungssysteme und die zu berücksichtigenden Faktoren.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

Schritt-für-Schritt-Anleitung

Bitten Sie die TeilnehmerInnen, ihre Gedanken zu den Vor- und Nachteilen der Verwendung alternativer Zahlungsmethoden zu teilen, und schreiben Sie sie auf die entsprechende Seite der Tafel (siehe obenstehende Beispiele).

Verwende hierfür das Whiteboard

Anleitung für den Trainer: Vor- und Nachteile

Aspekte wie Sicherheit, Benutzerfreundlichkeit, Kosten, Verfügbarkeit und mögliche Anreize stehen häufig im Mittelpunkt von Diskussionen über die Vor- und Nachteile verschiedener alternativer Zahlungssysteme. Indem diese Faktoren gründlich untersucht werden, verfügen die Lernenden über das erforderliche Wissen, um die Vor- und Nachteile der Verwendung alternativer Zahlungsmethoden abzuwägen. Dieses Verständnis erleichtert fundierte Entscheidungen über ihre Anwendung in verschiedenen finanziellen Angelegenheiten.

Die Verwendung alternativer Zahlungsmethoden bietet mehrere Vorteile. KundInnen haben beim Einkaufen eine größere Auswahl und Freiheit. Durch die Nutzung ihrer bevorzugten Zahlungsmethode können sie Unternehmen auch dabei unterstützen, KundInnen aus der ganzen Welt zu bewerben. Darüber hinaus können Unternehmen durch die Verwendung anderer Zahlungsoptionen ihre Kosten für die Abwicklung von Kreditkartenzahlungen möglicherweise senken.

Dennoch können bei der Nutzung alternativer Zahlungsoptionen einige Nachteile auftreten. KundInnen müssen beispielsweise möglicherweise mehrere Zahlungsalternativen zur Verfügung haben, da nicht alle Unternehmen alle Arten alternativer Zahlungsmethoden akzeptieren. Darüber hinaus bieten nicht alle anderen Zahlungsoptionen den gleichen Grad an Betrugsschutz wie Kreditkarten.

Aktivität 3: Sicherheit und Datenschutz bei der Verwendung alternativer Zahlungsmethoden.

Diese Aktivität zielt darauf ab, Datenschutz- und Sicherheitsbedenken im Zusammenhang mit der Nutzung alternativer Zahlungsmethoden anzusprechen. Sie erläutert die möglichen Gefahren bei der Verwendung verschiedener Zahlungsmethoden, darunter Betrug, Identitätsdiebstahl und Datenverletzungen. In der Diskussion wird die Bedeutung von präventiven Maßnahmen zur Verringerung dieser Risiken betont. Zu diesen präventiven Maßnahmen gehören das regelmäßige Überprüfen von Finanzauszügen auf Unregelmäßigkeiten, die Nutzung der Zwei-Faktor-Authentifizierung zum Schutz vor Kontenübernahmen und die Sicherstellung, dass Zahlungsempfänger legitim sind, bevor Geld überwiesen wird. Ziel ist es, VerbraucherInnen nützliche Taktiken zur Verringerung von Sicherheits- und Datenschutzproblemen bei der Nutzung anderer Zahlungsmethoden bereitzustellen.

Schritt-für-Schritt-Anleitung

Diskutieren Sie die Sicherheits- und Datenschutzimplikationen bei der Verwendung alternativer Zahlungsmethoden, wie das Risiko von Betrug, Datenlecks und Identitätsdiebstahl.

Fassen Sie die wichtigsten Punkte zusammen, die im Unterricht behandelt wurden, und betonen Sie die Bedeutung der sicheren und geschützten Verwendung alternativer Zahlungsmethoden.

Ermutigen Sie die TeilnehmerInnen, Fragen zu dem Thema zu stellen.

Leitfaden für den Trainer:

Die Einführung alternativer Zahlungssysteme hängt von der Sicherheit und dem Schutz der Privatsphäre ab. Es ist entscheidend, die Sicherheit dieser Techniken zu gewährleisten, um sich gegen Identitätsdiebstahl, Betrug und Verstöße gegen persönliche Informationen zu schützen. Es ist wichtig, die Verschlüsselungs- und Sicherheitsprotokolle zu verstehen, die diese Zahlungsoptionen schützen.

Betrugsrisiko: Alternative Zahlungsmethoden bieten neue Möglichkeiten für betrügerische Aktivitäten. Im Gegensatz zu traditionellen Zahlungssystemen können diese Methoden weniger strenge Sicherheitsmaßnahmen haben, was sie anfällig für unbefugte Transaktionen oder Kontenübernahmen macht. Benutzer müssen vorsichtig sein, wenn sie ihre Zahlungsinformationen teilen, und sich potenzieller Phishing-Versuche oder Betrugs bewusst sein.

Datenlecks: Alternative Zahlungsplattformen speichern sensible Finanzinformationen, wie Kreditkartendaten oder Kontonummern. Im Falle eines Datenlecks könnten diese Informationen kompromittiert werden, was zu finanziellen Verlusten und Identitätsdiebstahl führen könnte. Unternehmen, die alternative Zahlungsdienste anbieten, müssen robuste Sicherheitsmaßnahmen priorisieren, um Benutzerdaten vor unbefugtem Zugriff oder Cyberangriffen zu schützen.

Identitätsdiebstahl: Alternative Zahlungsmethoden erhöhen das Risiko von Identitätsdiebstahl, da sie oft von Benutzern persönliche Informationen anfordern, die für die Kontoerstellung und -verifizierung bereitgestellt werden müssen. Cyberkriminelle können Schwachstellen in diesen Systemen ausnutzen, um die Identitäten von Benutzern zu stehlen und betrügerische Aktivitäten durchzuführen. BenutzerInnen sollten beim Teilen persönlicher Informationen online vorsichtig sein und ihre Konten regelmäßig auf verdächtige Aktivitäten überwachen.

BenutzerInnen können ihre Privatsphäre stärken, informierte Entscheidungen treffen und Vertrauen in die Verwendung dieser Technologien entwickeln, indem sie sich der Sicherheitsverfahren und Datenschutzrichtlinien bewusst sind, die mit diesen Methoden verbunden sind. Das Unterkapitel zielt darauf ab, den TeilnehmerInnen jene Informationen zu geben, die sie benötigen, um die Sicherheits- und Datenschutzfunktionen mehrerer alternativer Zahlungsoptionen zu bewerten.

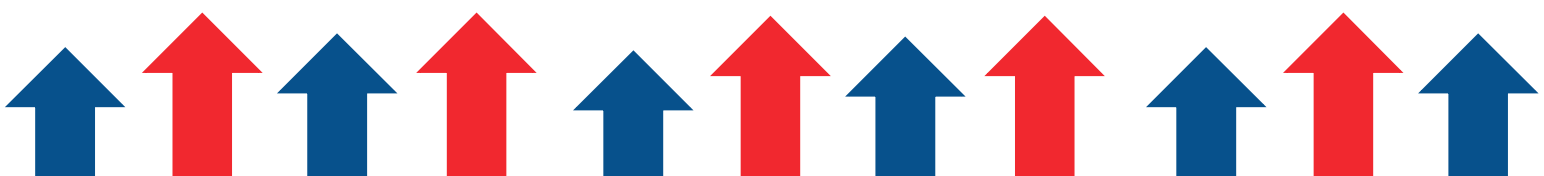
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

Diese Zahlungsmethoden bieten KundInnen mehr Auswahlmöglichkeiten und Flexibilität beim Einkaufen, aber es besteht die Möglichkeit, dass Betrug, Identitätsdiebstahl und Datenlecks auftreten.

Bei der Verwendung alternativer Zahlungsmethoden können KundInnen einige Sicherheitsmaßnahmen ergreifen, um diese Risiken zu verringern. Zum Beispiel sollten sie regelmäßig ihre Finanzauszüge überprüfen, um Unregelmäßigkeiten zu entdecken. Darüber hinaus müssen sie die Zwei-Faktor-Authentifizierung aktivieren, um sich gegen Datendiebstahl zu schützen. KundInnen sollten auch vor dem Senden von Geld das Ziel ihrer Zahlung bestätigen.

ZUSAMMENFASSUNG

Dieses Modul hat den TeilnehmerInnen grundlegende Kenntnisse und praktische Fähigkeiten im Bereich Online-Sicherheit und Finanzkompetenz vermittelt. Durch die Aufbereitung der Themen wie Online-Sicherheitsrisiken, sicheres Online-Shopping und alternative Zahlungsmethoden haben die TeilnehmerInnen Einblicke in die wirksame Sicherung persönlicher und finanzieller Informationen gewonnen. Das Modul zielt darauf ab, Einzelpersonen zu befähigen, informierte Entscheidungen zu treffen und sichere und nachhaltige finanzielle Praktiken im digitalen Zeitalter zu übernehmen.



REFERENZEN

- Anti-Phishing Working Group (APWG). (n.d.). Retrieved from https://www.apwg.org/
- Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). Retrieved from https://www.cisa.gov/
- Federal Trade Commission (FTC). (n.d.). Retrieved from https://www.ftc.gov/
- Grigutytė, M., & Grigutytė, M. (2023, December 27). Nigerian Prince scam: what is it and how it works. NordVPN. https://nordvpn.com/pt/blog/nigerian-prince-scam/
- Hayes, A. (2023, December 20). Bernie Madoff: Who He Was, How His Ponzi Scheme Worked. Investopedia. https://www.investopedia.com/terms/b/bernard-madoff.asp
- Krebs on Security. (n.d.). Retrieved from https://krebsonsecurity.com/
- SANS Institute. (n.d.). Retrieved from https://www.sans.org/
- Age Action. (n.d.). For All Older People. https://www.ageaction.ie
- Better Business Bureau. (2021). How to Protect Yourself When Shopping Online. https://www.bbb.org/article/tips/11205-bbb-tip-how-to-protect-yourself-when-shopping-online
- ESL Lesson Plans | Your English Pal. (2022, February 3). Your English Pal. https://www.yourenglishpal.com
- Federal Trade Commission. (2021). Online Shopping Tips. https://www.consumer.ftc.gov/articles/online-shopping-tips
- Get Safe Online | The UK's leading Online Safety Advice Resource. (2023, November 1). Get Safe Online. https://www.getsafeonline.org/)
- Kaspersky. (2021). Safe Online Shopping: 10 Tips to Avoid Scams. https://www.kaspersky.com/resource-center/online-safety/safe-online-shopping
- Norton. (2021). Online Shopping Safety Tips: How to Shop Online Safely. https://us.norton.com/internetsecurity-online-shopping-safety-tips-how-to-shop-online-safely.html
- Jackson, W. (2023, July 10). William Jackson | Data security policies: Necessary but not sufficient. Route Fifty. https://www.route-fifty.com/cybersecurity/2007/12/william-jackson-data-security-policies-necessary-but-not-sufficient/308532/
- K. (2023, March 10). Keeping Your money Safe Online. YouTube. https://www.youtube.com/watch?v=EL0_zRfpEnQ
- Marsh, L. (2023, November 3). How To Avoid Payment Fraud As A Property Manager. Forbes. https://www.forbes.com/sites/forbescommunicationscouncil/2023/11/03/how-to-avoid-payment-fraud-as-a-property-manager/?sh=455340a03362
- Mileva, G. (2023, October 26). Everything You Need to Know About Alternative Payment Methods in 2024. Influencer Marketing Hub. https://influencermarketinghub.com/alternative-payment-methods/
- Online Payment Processing Solution. (n.d.). GoCardless. https://gocardless.com/
- Payne, K. (2023, July 18). Axos Bank Review. Investopedia. https://www.investopedia.com/axos-bank-review-4802090
- What are the risks of digital payments? (2020, February 5). World Economic Forum. https://www.weforum.org/agenda/2015/02/what-are-the-risks-of-digital-payments/

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985

FinPower

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project Number: 2022-1-AT01-KA220-ADU-000087985