



Lerneinheit

[Schutz personenbezogener Daten in sozialen Medien]

Projekt: B-SAFE

Nummer: 2018-1CZ01-KA204-048148

Funded by the
Erasmus+ Programme
of the European Union



"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein."



Schutz personenbezogener Daten in sozialen Medien

Einführung

2010 machte die berühmte Comedy-Show Saturday Night Live einen Sketch über soziale Medien. Darin erklärte ein Schauspieler, der sich als Julian Assange (Gründer der Plattform WikiLeaks) ausgab, auf freudige und sarkastische Weise: "Ich gebe Ihnen kostenlos private Informationen über Unternehmen, und ich bin ein Bösewicht. Mark Zuckerberg [Gründer von Facebook] gibt Ihre Informationen an Unternehmen weiter, für Geld, und er ist [laut dem Time Magazine] Mann des Jahres. Sehen Sie einen Zusammenhang zwischen diesem Comedy-Sketch und der Realität? Was halten Sie davon, Ihre Daten einem Unternehmen kostenlos zur Verfügung zu stellen, während dieses damit Geld verdient? Sind unsere Daten sicher, während wir soziale Medien nutzen?"



Offensichtlich ist der Schutz personenbezogener Daten in sozialen Medien heutzutage ein sehr wichtiges Thema. Die Nutzung sozialer Medien nimmt exponentiell zu und ist heute für die Mehrheit der Menschen weltweit ein wesentlicher Bestandteil des täglichen Lebens. Von unserem Angestellten bis hin zu unserer lieben Großmutter nutzt fast jeder soziale Medien, um Fotos, Videos und Gespräche mit Freunden oder Verwandten zu teilen, persönliche Informationen insgesamt zu veröffentlichen und ein Gefühl der Nähe zu erzeugen.

Da die Nutzung sozialer Medien jedoch stark in unseren Gewohnheiten als Individuen und in der Gesellschaft verankert ist, lassen die meisten Menschen in Bezug auf die Cybersicherheit nach, was auf lange Sicht schwerwiegende Folgen haben kann.

Wer wird diese Daten noch sehen?

Daher gibt es viel über den Schutz von Daten und persönlichen Informationen bei der Nutzung sozialer Medien zu lernen, wie Sie in dieser Lerneinheit sehen werden.

Praktische Relevanz - Hierfür benötigen Sie das Wissen und die Fähigkeiten

Nachdem Sie sich durch diese Lerneinheit gearbeitet haben, werden Sie in der Lage sein, die wichtigsten Risiken in Bezug auf die Privatsphäre zu erkennen, die mit der Nutzung sozialer Netzwerke verbunden sind, und Sie werden wissen, wie Sie sich entsprechend schützen können.



1. Wissen aufbauen - Schutz personenbezogener Daten in sozialen Medien

Definition

Soziale Medien sind interaktive computervermittelte Technologien, die **die Schaffung oder den Austausch** von Informationen, Ideen, beruflichen Interessen und anderen Ausdrucksformen durch die Schaffung virtueller Gemeinschaften und Netzwerke erleichtern. Der Zweck der sozialen Medien besteht darin, sich **mit jedem Menschen auf der Erde oder mit vielen Menschen gleichzeitig zu verbinden und Informationen auszutauschen**. Sie können als Mittel zur Interaktion mit Freunden und Familie oder als Marketinginstrument von Unternehmen genutzt werden. Soziale Medien sind alle digitalen Werkzeuge, die es den BenutzerInnen ermöglichen, schnell Inhalte zu erstellen und mit anderen Menschen zu teilen.

In der obigen Box wird eine weit gefasste Definition von Social Media vorgestellt. Die Realität sieht so aus: Da es weltweit 3,5 Milliarden aktive Social-Media-NutzerInnen gibt, haben sich die sozialen Medien in einer Weise entwickelt, dass sie derzeit in verschiedene Kategorien unterteilt sind, was die Interessen und Absichten der NutzerInnen betrifft. Als nächstes wird eine Liste von 10 Arten von Social Media vorgestellt, je nach ihrer Zielsetzung:

	Zweck	Beispiel
Social Networks	Mit Menschen (und Marken) online in Verbindung treten	   Facebook; Twitter; LinkedIn
Netzwerke zur gemeinsamen Mediennutzung	Fotos, Videos, Live-Videos und andere Medien online finden und mit anderen teilen	   Instagram; Youtube; Tik Tok
Diskussionsforen	Nachrichten, Informationen und Meinungen finden, diskutieren und austauschen	  Reddit; Quora
Netzwerk für Inhaltskuratoren	Neue und zukunftsweisende Inhalte und Medien entdecken, speichern, teilen und diskutieren	  Pinterest; Flipboard
Netzwerk für Verbraucherprüfungen	Informationen über Marken, Produkte und Dienstleistungen sowie über Restaurants, Reiseziele usw. zu finden, zu prüfen und auszutauschen	   Yelp; Zomato, Tripadvisor
Blogging- und Publishing-Netzwerk	Inhalte online veröffentlichen, entdecken und kommentieren	  Wordpress; Tumblr
Soziales Einkaufsnetzwerk	Um Trends zu erkennen, Marken zu folgen, große Funde zu teilen und Einkäufe zu tätigen	 Etsy



Interessengebundenes Netzwerk	Sich mit anderen, durch ein gemeinsames Interesse oder Hobby zu verbinden.	  Goodreads; Last.Fm
"Netzwerk "Wirtschaft teilen"	Produkte und Dienstleistungen zu bewerben, zu finden, zu teilen, zu kaufen, zu verkaufen und zwischen Gleichaltrigen zu tauschen	   Airbnb; Uber; Glovo
Anonymes soziales Netzwerk	Gedanken austauschen, Ratschläge zu geben, über den neuesten Klatsch und Tratsch plaudern	  Whisper; Ask.fm

Es besteht kein Zweifel, dass wir im Zeitalter der sozialen Medien leben. Aus diesem Grund gibt es zahlreiche rechtliche Fragen zu sozialen Medien, die entstehen, wenn Menschen Inhalte online über verschiedene Plattformen wie Instagram, Pinterest, Facebook und so weiter austauschen. Die wichtigsten Rechte im Bereich der sozialen Medien beziehen sich darauf, wem die geteilten Inhalte gehören, wann und wo die gemeinsame Nutzung angemessen ist und welche Grenzen der gemeinsamen Nutzung auferlegt werden können, und werfen oft Fragen in Bezug auf Marken- und Urheberrechtsverletzungen, Marketing in sozialen Medien, Arbeitsbeziehungen und vieles mehr auf. Hier finden Sie eine kurze Auflistung der wichtigsten Social-Media-Rechte für Instagram, WhatsApp, Youtube und Facebook.



1. Offiziell besitzen Sie jedes Bild und/oder Video, das Sie veröffentlichen, aber andere Personen könnten für die Nutzung bezahlen, und Instagram wird Ihnen dafür nichts bezahlen.
2. Sie sind verantwortlich für alles, was Sie mit Instagram tun und was Sie veröffentlichen.
3. Obwohl Sie für die Informationen, die Sie in diesen sozialen Medien veröffentlichen, verantwortlich sind, kann Instagram persönliche Informationen aufbewahren, verwenden und an mit Instagram verbundene Unternehmen weitergeben.
4. Sie können Ihr Instagram-Konto schließen. Wenn Sie dies tun, werden Ihre Fotos, Beiträge und Ihr Profil aus Ihrem Konto verschwinden, aber wenn jemand Ihre Fotos oder persönlichen Daten freigegeben hat, oder wenn jemand diese Art von Informationen aus irgendeinem Grund verwendet, können sie immer noch in diesen sozialen Medien erscheinen.



1. Sie können Ihren Profilnamen, Ihr Bild und Ihre Statusmeldung jederzeit ändern
2. Jeder, der WhatsApp verwendet, kann möglicherweise Ihre Mobiltelefonnummer, Ihren Profilnamen, Ihr Foto, Ihren Status, Ihre Statusmeldung, Ihren zuletzt gesehenen Status und Ihren Nachrichtenerhalt sehen. Sie können dies ändern, wenn Sie möchten, und Sie können auch Ihre Einstellungen verwenden, um Personen zu blockieren und zu steuern, mit wem Sie chatten.
3. Nachdem Ihre Nachrichten zugestellt wurden, löschen wir sie aus unserem System und sie werden nur auf Ihrem eigenen Telefon oder Gerät gespeichert. Ihre Nachrichten sind "verschlüsselt", was bedeutet, dass die Firma, die WhatsApp besitzt, sie nicht lesen kann.
4. Andere Unternehmen dürfen keine Werbung auf Ihrem WhatsApp Bildschirm platzieren, es sei denn, Sie sind mit ihnen verbunden.



- | |
|---|
| 1. Wenn Sie ein YouTube-Konto erstellen, werden Ihre Daten von Google erfasst. Sie können entscheiden, ob Youtube einige dieser Informationen erfassen soll, indem Sie zu Ihrem Google-Konto "Aktivitätskontrollen" gehen. Darüber hinaus bleiben Ihre persönlichen Daten ohne Ihre Zustimmung innerhalb der Google-Unternehmen |
| 2. Sie können Youtube um die Informationen bitten, die dort über Sie gespeichert sind, und Sie können das Unternehmen bitten, diese zu korrigieren oder zu löschen. |
| 3. Wenn Sie sich über Ihren Auftritt in einem Youtube-Video beschweren möchten, können Sie Youtube die URL des Videos mitteilen, die genaue Uhrzeit angeben, zu der Sie oder Ihre Informationen im Video erscheinen, und erklären, warum Sie sich von anderen Personen im Video abheben |
| 4. Wenn sich jemand über ein Video beschwert, das Sie in Ihrem Channel haben, und Youtube mit ihm einverstanden ist, werden Sie benachrichtigt, dass Sie das Video herunterladen oder seine persönlichen Daten bearbeiten müssen. |



- | |
|--|
| 1. Auch wenn Ihr Profil privat ist, denken Sie bitte daran, dass andere Personen Informationen sehen und weitergeben können, die andere über Sie veröffentlichen. Andere Personen können auch Informationen, die Sie über sich selbst gepostet haben, auf ihren eigenen Telefonen und Geräten speichern. |
| 2. Einige Unternehmen werden Informationen über Sie mit Facebook teilen und Facebook wird Informationen über Sie mit ihnen teilen |
| 3. Wenn Sie der Verwendung einer Anwendung auf Facebook zustimmen, kann diese Anwendung möglicherweise die Informationen, die Sie auf Facebook veröffentlichen, verwenden, teilen und behalten. |
| 4. Wenn Sie Ihr Konto löschen, werden Dinge, die Sie gepostet haben, gelöscht, nicht aber Dinge, die andere Personen über Sie mitgeteilt haben. |

1.1.Wissen anwenden

Übung MULTIPLE CHOICE

Situation: Was sind "Soziale Medien"?

Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Website und Anwendungen, die es Menschen ermöglichen, Nachrichten und Fotos zu versenden.
- Soziale Medien sind eine Form der elektronischen Kommunikation (z.B. Websites für soziale Netzwerke).
- Websites und Computerprogramme, die es Menschen ermöglichen, über das Internet mit Hilfe eines Computers oder Mobiltelefons zu kommunizieren und Informationen auszutauschen.
- Soziale Medien beziehen sich auf Websites und Anwendungen, die so gestaltet sind, dass Inhalte schnell ausgetauscht werden können.

Übung MULTIPLE CHOICE



Situation: Welche Rechte zum Schutz personenbezogener Daten werden in WhatsApp angewendet?

Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Sie haben das Recht auf verschlüsselte Nachrichten, was bedeutet, dass WhatsApp die Nachrichten, die Sie an andere Personen senden, nicht lesen kann.
- Sie haben das Recht, Ihren WhatsApp-Account zu löschen, was bedeutet, dass die Nachrichten, die Sie an andere Personen gesendet haben, nicht mehr gelesen werden können.
- Wenn Sie nur die Anwendung WhatsApp auf Ihrem Gerät löschen, aber den Account nicht löschen, bleiben die Informationen erhalten.
- WhatsApp speichert und bewahrt Informationen über Sie auf, kann Ihre Informationen aber nicht überall auf der Welt verwenden.

2. Wissen aufbauen - Häufigste Risiken in sozialen Medien

Heutzutage ist es allgemein bekannt, dass soziale Medien unsere täglichen Interessen und Aktivitäten integrieren. Teilen wir jedoch die Gewohnheiten und Verhaltensweisen hinsichtlich der Nutzung sozialer Medien? Um die Relevanz von Social Media in unserer Gesellschaft zu verstehen, ist es wichtig, dass wir auf dem neuesten Stand der Social-Media-Statistiken bleiben. Als nächstes präsentieren wir die 10 relevantesten Statistiken zu sozialen Medien:

DIE 10 RELEVANTESTEN STATISTIKEN FÜR SOCIAL MEDIA



73% der MarketingexpertInnen glauben, dass Social Media Marketing sehr effektiv für ihr Unternehmen war (Buffer, 2019)



3,5 Milliarden aktive Social-Media-Nutzer weltweit, was 45% der Bevölkerung entspricht (Emarsys, 2019)



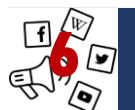
Die Zahl der täglich aktiven NutzerInnen von Instagram Stories stieg von 150 Millionen im Januar 2017 auf 500 Millionen täglich aktive Stories weltweit im Januar 2019 (Buffer, 2019)



Facebook bleibt die am weitesten verbreitete soziale Medienplattform (Pewinternet, 2018)



91% aller NutzerInnen sozialer Medien greifen über mobile Geräte auf soziale Kanäle zu (Buffer, 2019)



71% der VerbraucherInnen wollen, bei sozialen Plattformen mit Marken darauf drängen, ihre persönlichen Daten besser zu schützen (Edelman, 2008)



91% aller NutzerInnen sozialer Medien greifen über mobile Geräte auf soziale Kanäle zu (Buffer, 2019)



Digitale KonsumentInnen verbringen fast 3 Stunden pro Tag mit sozialen Netzwerken und Messaging (Globalwebindex, 2018)



81% der kleinen und mittleren Unternehmen nutzen derzeit soziale Medien, um das Unternehmenswachstum voranzutreiben, und 9% planen, sie in Zukunft zu nutzen (LinkedIn, 2014)



Im Durchschnitt verfügen die Menschen über 7,6 Social-Media-Konten (Clement, 2019)

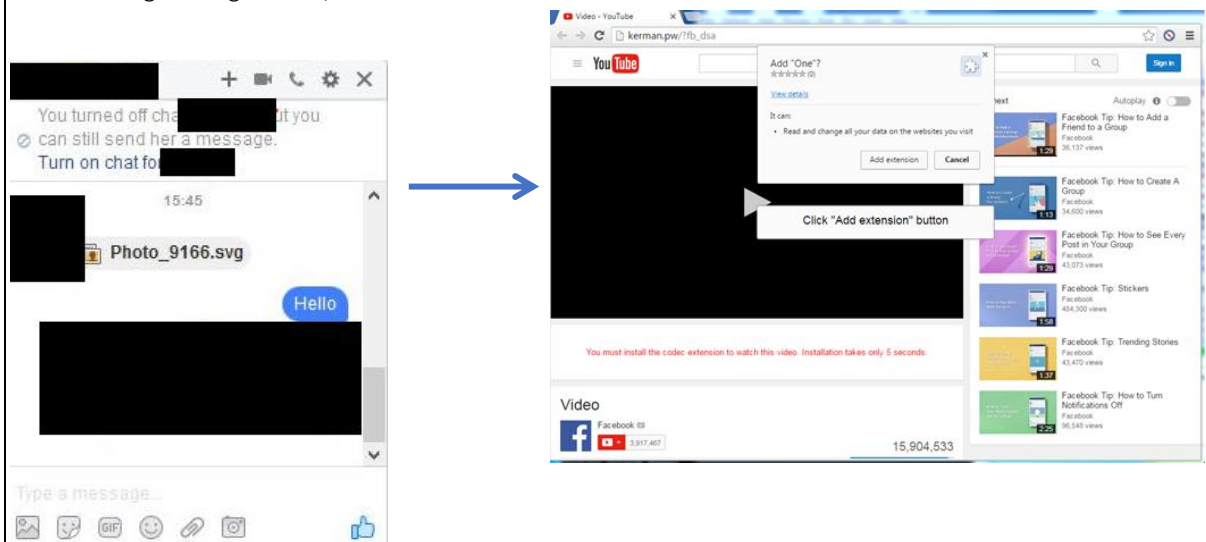
Bei dieser Art von Statistiken ist es kein Wunder, dass soziale Mediennetzwerke zu einer der berühmten Plattformen für das Sammeln von Benutzerdaten werden, die entweder vom Netzwerk selbst auf legale Weise oder von Hackern in böswilliger Absicht aufrechterhalten werden.

Das stärkste Risiko der sozialen Medien ist Malware, die alle Ihre Daten kompromittieren kann. Es gibt verschiedene Arten von Malware mit unterschiedlichen Zwecken, wie Sie unten sehen können:

1. **Erpressungs-Software**, die Verschlüsselung verwendet, um den Zugriff eines Ziels auf seine Daten, wie Fotos oder Dokumente, zu sperren, bis ein Lösegeld gezahlt wird. Diese Malware wird aktiviert, wenn der Benutzer bzw. die Benutzerin auf einen Hyperlink klickt, der in einer Social-Media-Plattform veröffentlicht wurde, oder auf ein Bild, das den Benutzer bzw. die Benutzerin auf eine externe Website umleitet, die den bösartigen Code verbreitet.

Beispiel für eine Erpressungs-Software

Chat-Anwendungen wie WhatsApp oder Facebook Messenger sind gängige Mittel für Lösegeld-Angriffe. In diesem Beispiel sendeten Cyberkriminelle über Facebook Messenger betrügerische Nachrichten mit SVG-Bildanhängen. NutzerInnen, die auf das Bild klickten, fanden sich selbst auf einer Website, die ein Popup-Fenster zur Installation einer Browsererweiterung oder eines Add-ons zur Anzeige eines Videos aufrief. Später, nachdem der bösartige Code das System des Nutzenden infiziert hatte, erschien ein weiteres Popup, in dem eine Zahlung verlangt wurde, um die Dateien des Nutzenden freizuschalten.





2. **Trojanisches Pferd** - Art von bösartigem Code oder Software, die legitim aussieht, aber die Kontrolle über Ihren Computer übernehmen kann. Ein Trojaner ist darauf ausgelegt, Daten zu stehlen (Logins, Finanzdaten, sogar elektronisches Geld), mehr Malware zu installieren, Dateien zu modifizieren, Benutzeraktivitäten zu überwachen (Screen Watching, Keylogging usw.), den Computer in Botnetzen zu verwenden und die Internetaktivitäten des Angreifers bzw. der Angreiferin zu anonymisieren. Ein Trojaner verhält sich wie eine legitime Anwendung oder Datei, um Sie zum Herunterladen und Installieren von Malware zu verleiten. Einmal installiert, kann ein Trojaner die Aktion ausführen, für die er konzipiert wurde.
In der Regel ist ein Trojaner in gefälschter Werbung versteckt oder wird per Instant Messaging an Nutzenden gesendet.
3. **Virus** - Form von Malware, die in der Lage ist, sich selbst zu kopieren und auf andere Computer zu verbreiten. Viren verbreiten sich häufig auf andere Computer, indem sie sich an verschiedenen Programmen anhängen und Codes ausführen, wenn ein Benutzer bzw. eine Benutzerin eines dieser infizierten Programme startet. Viren können sich auch über Skriptdateien, Dokumente und Cross-Site-Scripting-Schwachstellen in Webanwendungen verbreiten. Viren können verwendet werden, um Informationen zu stehlen, Host-Computer und Netzwerke zu schädigen, Botnetze zu erstellen, Geld zu stehlen, Werbung zu übertragen und vieles mehr.
4. **Greyware** - Form von Malware, die Ihren Daten nicht wirklich physischen Schaden zufügt, wie es andere Malware kann, und die sich in einer lästigeren Form präsentiert, wie Adware und Spyware. Sie hat eine hohe Verbreitung in sozialen Medien, normalerweise in Form von "Klick-Ködern", bei denen ein verlockender Artikel Sie zu einer Website führt, die Sie zu einer Aktion auffordert, z. B. zur Installation eines gefälschten Social-Media-Plugins oder zum Ausfüllen einer schnellen Umfrage, bevor Sie auf die Medien zugreifen. Diese Informationen werden dann gesammelt und an andere Cyberkriminelle verkauft und können bei Versuchen, sich in Ihre persönlichen Konten zu hacken, verwendet werden.

Beispiel für Greyware

Im Laufe der Jahre haben BetrügerInnen sowohl echte als auch gefälschte Todesfälle unter Prominenten als Mittel benutzt, um BenutzerInnen davon zu überzeugen, auf Links zu klicken und Aktionen durchzuführen.

Ein berühmtes Beispiel war der Tod des Schauspielers Robin Williams im Jahr 2014. Nur 48 Stunden nach seinem Tod kam in Facebook ein Video in Umlauf, das angeblich einen Link zu einem angeblichen Abschiedsvideo von Williams enthielt. BenutzerInnen, die auf den Link zu dem angeblichen Video klickten, wurden zu einer gefälschten BBC-Nachrichten-Website geleitet. Dann wurden sie angewiesen, das Video vor dem Ansehen auf Facebook weiterzugeben. Nachdem sie die Seite wie gewünscht freigegeben hatten, erschien eine zweite gefälschte Seite und forderte das Ausfüllen einer Online-Umfrage. Persönliche Informationen wurden gesammelt und dann an skrupellose Internet-Vermarkter verkauft.



5. **Würmer** - Würmer gehören zu den häufigsten Arten von Malware. Würmer können Dateien verändern und löschen, Daten stehlen, eine Hintertür installieren und es einem Hacker ermöglichen, die Kontrolle über einen Computer und seine Systemeinstellungen zu erlangen. Sie können sogar zusätzliche bösartige Software in einen Computer einschleusen. Würmer können über Software-Schwachstellen übertragen werden oder als Anhänge in Spam-E-Mails oder Instant Messages ankommen. Einmal geöffnet, könnten diese Dateien einen Link zu einer bösartigen Website enthalten oder den Computervorm automatisch herunterladen. Sobald er installiert ist, geht der Wurm unbemerkt an die Arbeit und infiziert den Computer ohne das Wissen des Benutzers bzw. der Benutzerin. Würmer verbreiten sich häufig, indem sie Massen-Sofortnachrichten mit infizierten Anhängen an die Kontakte der Nutzenden senden.

Wie Sie feststellen können, verwendet all diese Malware die gleiche Strategie, um den Nutzenden anzulocken, nämlich Phishing-Betrügereien oder Angriffe. **Phishing-Angriffe** nutzen bösartige Quellen, um persönliche und finanzielle Informationen zu sammeln oder den Rechner des Nutzenden mit Malware zu infizieren.

Der erste Schritt bei einem Phishing-Anhang ist immer derselbe: In Ihrem Social Media Feed oder in Ihrer Instant Message-Anwendung erscheint ein Link, ein Foto, ein Video, ein Artikel oder eine Werbung. Dies kann von jedermann stammen - von einer Nachrichtenquelle, einem Prominenten, einem Unternehmen, dem sozialen Netzwerk selbst oder sogar von einem vertrauenswürdigen Kontakt. Meistens handelt es sich bei diesen Quellen um Nachahmer realer Konten oder um Nutzende, deren Social-Media-Konto kompromittiert oder deren Identität gestohlen wurde.

Beispiel für einen Fake Account

Twitter verfügt über ein Werkzeug, das Konten verifiziert, um betrügerische Aktivitäten zu reduzieren, genannt "Twitter Verified". Dies ist das eigentliche Konto dafür:



Co-funded by the
Erasmus+ Programme
of the European Union



Es dauerte nicht lange, bis ein Klon-Account auftauchte, der behauptet, der authentische Verifizierungshilfe-Account zu sein, und die NutzerInnen zu allen möglichen bösartigen Nutzlasten leitet.

Social Media Phishing spielt mit Ihren grundlegenden menschlichen Emotionen und Bedürfnissen, wie Vertrauen, Sicherheit, Trauer, Angst vor Geldverlust, Angst, etwas umsonst zu bekommen, Eifer nach einem Schnäppchen oder der Wunsch, Liebe oder Popularität/Status zu finden. Im Allgemeinen erklären oder implizieren sie auch die Notwendigkeit Ihres dringenden Handelns, um entweder ein Problem zu vermeiden oder ein Angebot zu nutzen.

Beispiele für Phishing-Betrügereien

Beispiele für Phishing-Betrügereien

- **OMG! Haben Sie dieses Bild von Ihnen gesehen?**
- **Geheime Details über Michael Jacksons Tod!**
- **Nur 1% der Menschen können dieses Problem lösen! Machen Sie jetzt das Quiz!**
- **Adidas verschenkt zur Feier seines 93. Jubiläums 3.000 Gratis-Schuhe. Holen Sie sich jetzt Ihre Gratis-Schuhe!**

Dabei handelt es sich um sehr häufige Phishing-Betrügereien, die eine Frage, einen Prominenten, eine Marke oder eine Tatsache betreffen, die das Interesse des Benutzers bzw. der Benutzerin wecken und ihn dann auf einen gefälschten Anmeldebildschirm leiten, um Login-Informationen zu erhalten, oder die automatisch Malware auf einem Computer installieren.

Der zweite Schritt eines Phishing-Angriffs besteht darin, den Nutzenden auf eine Website umzuleiten, die vertrauliche Details anfordert oder Ihren Computer oder Ihr mobiles Gerät mit Malware infiziert. Diese Malware kann automatisch oder nach Aufforderung zum Download eines Programms, einer Browser-Erweiterung oder einer Anwendung installiert werden.



Alternativ können Sie durch die Post, den Tweet oder die Nachricht angewiesen werden, einen Telefonanruf an eine bestimmte Nummer zu tätigen. Dies kann entweder dazu führen, dass vertrauliche Details angefordert werden oder dass Ihrer Telefonrechnung exorbitante Gebühren auferlegt werden.

2. Wissen anwenden

Übung MULTIPLE CHOICE

Situation: Welche Aussage ist falsch?

Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Soziale Medien sind ein wirksames Marketinginstrument für Unternehmen
- Facebook ist die meistgenutzte soziale Medienplattform
- Die meisten Nutzer sozialer Medien greifen über mobile Geräte auf soziale Kanäle zu
- Kleine und mittlere Unternehmen nutzen derzeit soziale Medien, um das Unternehmenswachstum voranzutreiben
- Die Benutzer neigen dazu, sich für ein soziales Netzwerk zu entscheiden und es täglich zu nutzen.

Übung SINGLE CHOICE

Situation: Sie scrollen durch Facebook und sehen die folgende Publikation:



Was würden Sie tun?

Aufgabe: Wählen Sie die richtige Option nach dem Multiple-Choice-Prinzip aus: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- OMG, heute ist mein Glückstag! Ich klicke auf "WEITER" und gebe ihnen alle notwendigen Daten, um die Geschenkkarte zu gewinnen. Danach teile ich die Gelegenheit mit all meinen Cyber-Freunden!
- Ich habe nur 4 Minuten, um meinen Preis einzufordern! Ich klicke auf "WEITER" und gebe ihnen alle notwendigen Daten, um den Preis zu gewinnen. Aber nachdem ich gesehen habe, dass ich Bankdaten angeben muss, gebe ich auf. Zu viel Arbeit.
- Ich werde neugierig und klicke auf "WEITER". Nachdem ich gesehen habe, dass es notwendig ist, ihnen persönliche Daten mitzuteilen, schließe ich die Registerkarte. Ich denke, es ist ein Betrug.
- Ich klicke nicht in die Publikation. Ich kann keine Lotterie gewinnen, an der ich nie teilgenommen habe! Ich melde den Beitrag an Facebook als "Betrug".



3. Wissen aufbauen - einige Sicherheitstipps zur Verwendung von Social-Media-Konten



Nun, da Sie die vielfältigen Risiken der Nutzung sozialer Netzwerke kennen, glauben Sie bitte nicht, dass die einzige Lösung zur Gewährleistung Ihrer Sicherheit und Ihrer Privatsphäre die Löschung Ihrer sozialen Konten ist! Das Geheimnis besteht darin, soziale Medien zu nutzen und gleichzeitig die Risiken zu verstehen und zu wissen, wie man sich entsprechend verhält.

Es gibt einige übliche Verhaltensweisen von BetrügerInnen und HackerInnen, die uns auf die Möglichkeit eines Phishing-Betrugs aufmerksam machen können. Wenn Sie in Ihrem bevorzugten sozialen Mediennetzwerk surfen, achten Sie immer auf diese roten Flaggen, die darauf hinweisen, dass es sich bei dem Beitrag um einen Phishing-Betrug handelt:

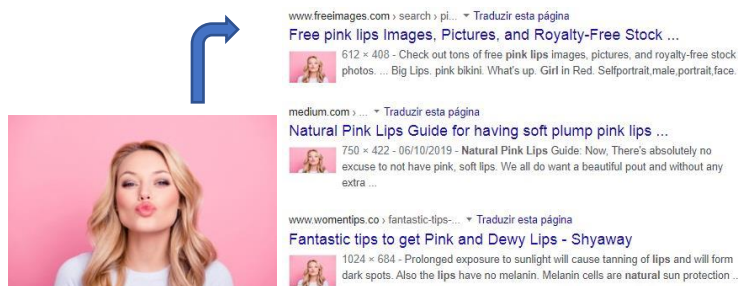
Rote Flagge #1: Freundschaftsanfragen von Fremden

Sie haben eine Freundschaftsanfrage von einem Fremden erhalten? Jemand, den Sie nicht kennen, hat Ihnen eine private Nachricht geschickt? Ein Unternehmen oder eine Persönlichkeit des öffentlichen Lebens hat Sie gebeten, ihnen zu folgen?

Plattformen wie Facebook, Instagram und Twitter sind voll von gefälschten Profilen mit der Absicht von Phishing-BenutzerInnen. Akzeptieren Sie keine Freundschaftsanfragen ohne Überprüfung. Wenn Sie jemand stört, ist es gut, solche Profile zu melden und zu blockieren.

Tipp

Führen Sie eine umgekehrte Bildsuche des Profilfotos durch. In den meisten Fällen verwenden HackerInnen Stockfotos. Wenn Sie Ergebnisse für verschiedene Websites haben, die dieses Foto für unterschiedliche Zwecke verwenden, handelt es sich um ein gefälschtes Konto.





Tipp

Haben Sie schon einmal das blaue Häkchen neben den Namen bekannter Persönlichkeiten oder Unternehmen auf sozialen Plattformen bemerkt? Es sieht so aus:

- Twitter: • **Stephen King** ✓
- Facebook: • **adidas** ✓
- Instagram: • **cristiano** ✓

Dieses Häkchen ist in fast jeder sozialen Medienplattform vorhanden und bedeutet, dass das **Konto** als authentisch **verifiziert** ist und einer prominenten Person oder Branchenführer bzw. Branchenführerin gehört.

Wenn Sie zum Beispiel eine Nachricht von einem "Twitter Verified"-Account ohne das Häkchen erhalten, passen Sie auf - es handelt sich wahrscheinlich um eine Fälschung!

Redflag #2: Klicken Sie auf diesen Link!

Das Ziel eines Phishing-Angriffs ist es in der Regel, Sie dazu zu bringen, einen Anhang herunterzuladen (z.B. ein Foto, das in einer direkten Nachricht gesendet wurde) oder auf einen Link zu klicken. Manchmal geben sich Kriminelle als vertrauenswürdige Quellen aus, um Sie dazu zu bringen, auf einen Link zu klicken (oder eine Anwendung herunterzuladen), die Malware enthält. Was wie ein legitimer Hyperlink aussieht, kann ein getarnter Link zu einer kriminellen Website sein.

Klicken Sie daher nicht auf einen Link, der Sie auf eine andere Website weiterleitet. Gehen Sie stattdessen direkt zur Quelle - Markenwebsite, Bankseite usw. - und bestätigen Sie, ob Sie in den sozialen Medien sehen, dass es sich um echte Werbung oder Ankündigung handelt.

Tipp

Eine schnelle Möglichkeit, um zu überprüfen, ob der Hyperlink Sie zu einer vertrauenswürdigen Quelle weiterleitet, besteht darin, mit der Maus über den Text des Hyperlinks zu fahren. Sie sollten die vollständige URL sehen, die Ihnen hilft zu zeigen, ob sie zu einer legitimen Website führt.

Please follow the link below and login to your account
and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

Sincerely,

Paypal customer department

<http://66.160.154.156/catalog/paypal/>

Was ist der wichtigste Hinweis, den wir suchen sollten, die URL?

Achten Sie bitte auf den Anfang der URL: sichere URLs beginnen mit "https" statt nur mit "http", um anzuzeigen, dass sie verschlüsselt sind. Das "s" in "https" steht für "sicher". Dieser Hyperlink ist also ein Phishing-Betrug!

Tipp

Was ist, wenn Sie auf einen Link klicken? Was sollten Sie dann tun?

Wenn dieser Link Sie auf eine Website weiterleitet, gibt es ein paar Anzeichen, nach denen Sie Ausschau halten können, damit Sie wissen, ob es ein Unternehmen gibt oder nicht.

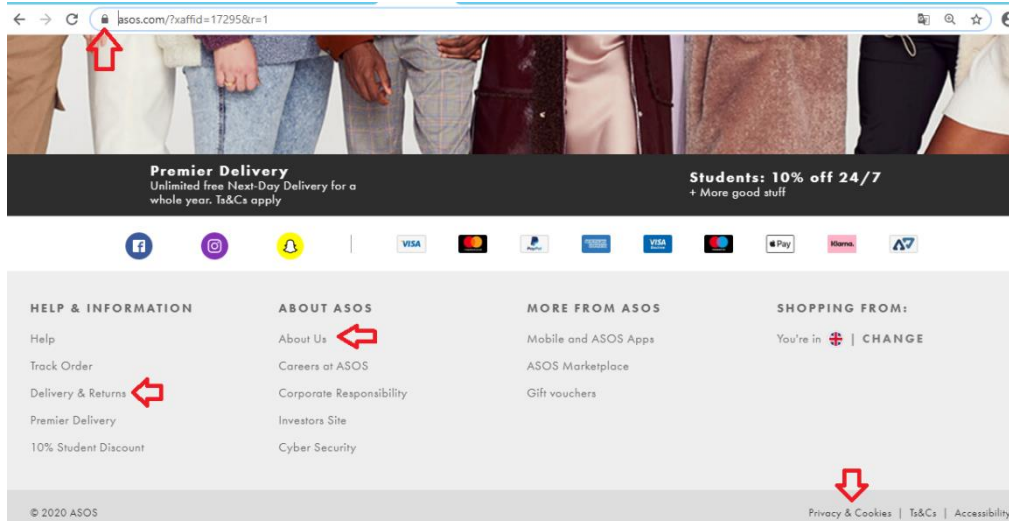
Bevor Sie also irgendetwas tun, z.B. Ihre Anmeldedaten eingeben oder auf den Download-Button klicken, sollten Sie nach diesen Hinweisen suchen:

- In der Suchleiste erscheint "https" oder ein "Schloss"-Symbol - das bedeutet, **dass die Website gesichert ist.**



Co-funded by the
Erasmus+ Programme
of the European Union

- **Schauen Sie sich die Domain an** - Cyber-Angreifer sind sehr hinterhältig. In den meisten Fällen sind die Domains der echten sehr ähnlich, zum Beispiel "as0s.com" oder "asos.net".
- **Es gibt eine physische Adresse und eine Telefonnummer** - seriöse Firmen werden ihre Informationen auflisten, damit Sie sie bei Problemen kontaktieren können.
- **Rückgabe-Richtlinien** - seriöse Websites sollten ihre Rückgabe-Richtlinien sowie ihre Versand-Richtlinien auflisten.
- **Datenschutzerklärung** - Seriöse Websites sollten Ihnen mitteilen, wie sie Ihre Daten schützen und ob sie Ihre Daten an Dritte weitergeben.



Redflag #3: Beförderungen und Wettbewerbe zu schön, um wahr zu sein!

Dies ist ein sehr häufiger Phishing-Betrug. Durch die Präsentation sehr niedriger Preise, das Anbieten unwiderstehlicher Preise oder das Verschenken von Rabatten können BetrügerInnen BenutzerInnen dazu verleiten, private Informationen preiszugeben.

Tipp

Was sind die üblichen Anzeichen für einen Wettbewerbsbetrug?

- Die soziale Seite hat eine niedrige Follower-Zahl;
- Schlechte Grammatik und Rechtschreibung;
- Sie bitten um sehr persönliche Informationen, wie den Namen Ihrer Mutter, Ihr erstes Haustier, ob Sie Kinder haben, usw. Alles, was sie wollen, sind Hinweise, um Ihr Passwort zu knacken!
- - Sie sind sehr hartnäckig in ihrem Dialog! Sie wollen nur, dass Sie das Gefühl der "Dringlichkeit" spüren.

Wie Sie feststellen können, gibt es Möglichkeiten, Phishing-Betrügereien in sozialen Medien aufzudecken und so zu verhindern, dass Sie Opfer eines Cyberattacks werden, der Ihre persönlichen Daten kompromittiert. Aber ein aufmerksames Auge zu haben, reicht nicht aus. Im Hinblick auf Cyberattacken ist die beste Abhilfe die Prävention. Was können Sie also tun, um Cyberkriminellen in den sozialen Medien immer einen Schritt voraus zu sein?



Überprüfen Sie Ihre Datenschutzeinstellungen

Zuverlässige soziale Mediennetzwerke ermöglichen es Ihnen, die Datenschutzeinstellungen auf ein für Sie angenehmes Niveau einzustellen. Welche Art von Informationen möchten Sie veröffentlichen? Ihre Fotos? Ihre Hobbys? Und mit wem möchten Sie diese Informationen teilen? Ihren Freunden in sozialen Netzwerken oder allen anderen?

Wenn Sie die Privatsphäre-Einstellungen ändern, können Sie Fremden und Personen, die nicht Ihre Freunde sind, die Anzeige Ihres Profils und der von Ihnen freigegebenen Informationen untersagen.

Um dies zu tun, sollten Sie die "Definitionen" Ihres Social-Media-Kontos überprüfen.



Sicherheitssoftware auf dem neuesten Stand halten

Die neueste Sicherheitssoftware, der neueste Webbrowser und das neueste Betriebssystem sind die beste Verteidigung gegen Viren, Malware und andere Online-Bedrohungen.

Sie können in Ihrem Browser auch eine Erweiterung installieren, die unerwünschte Werbung blockiert.



Sichere Passwörter

Die Erstellung eines sicheren Passworts verhindert, dass Hacker Zugang zu Ihrem Konto erhalten und es zum Versenden von Spam oder böswilligen Angriffen verwenden können. Ein sicheres Passwort hat nicht weniger als 8 Zeichen und besteht sowohl aus Buchstaben als auch aus Zahlen. Es sollte außerdem alle 3 Monate geändert werden und für jedes Konto eindeutig sein.

Tipp: Verwenden Sie anstelle eines Passworts eine Passphrase, zum Beispiel "IAte27P0tat0s".



Behalten Sie Ihre Geheimnisse für sich

Vermeiden Sie es, persönliche Daten online weiterzugeben, denn Ihre Informationen, einschließlich Ihrer E-Mail-Adresse, Telefonnummer und Sozialversicherungsnummer, sind HackerInnen und Data-Mining-Unternehmen eine Menge Geld wert. Diese Daten könnten für Lösegeld, Identitätsdiebstahl oder als Hinweis zum Erraten Ihrer Passwörter verwendet werden.

Werfen Sie einen Blick auf Ihre Social-Media-Profile und versuchen Sie, es möglichst anonym zu halten - die Leute, die Ihr Geburtsdatum, Ihre E-Mail-Adresse und Ihre Telefonnummer kennen müssen, haben sie bereits.



VPN verwenden

Wenn Sie Ihre Gespräche, Nachrichten und Anrufe sicher halten wollen, können Sie ein Virtual Private Network (VPN) verwenden. Ein VPN ist ein verschlüsselter Tunnel zwischen zwei Geräten, über den Sie privat und sicher auf alle Websites und Online-Dienste zugreifen können.

Da die Daten verschlüsselt sind, können HackerInnen, Behörden und sogar InternetdienstanbieterInnen Ihre Informationen nicht sehen oder die Kontrolle über sie erlangen, während Sie mit einem VPN-Server verbunden sind. Es gibt eine Vielzahl von VPN-AnbieterInnen online, und sie unterscheiden sich in Bezug auf Preise und Anpassung.



Vergessen Sie nicht, sich abzumelden

Denken Sie an diese goldene Regel: Melden Sie sich immer von allen Ihren Social-Media-Plattformen ab, wenn Sie sie nicht mehr benutzen. Wenn Sie sich nicht abmelden, erlauben Sie jedem, der Zugang zu Ihrem Computer hat, legal oder nicht, den Browser oder die Anwendung zu öffnen und sofortigen Zugang zu Ihren Konten auf solchen Seiten zu haben, ohne Passwörter oder Benutzernamen einzugeben.

3. Wissen anwenden

Übung MULTIPLE CHOICE

Situation: Was sind die Anzeichen für einen möglichen Phishing-Betrug, dass Sie beim Surfen in sozialen Medien immer wachsam sein müssen?

Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Grammatik und Rechtschreibung der Veröffentlichung.
- Das Vorhandensein von Hyperlinks: Nur eine glaubwürdige Quelle kann einen Link zu ihrer Website veröffentlichen.
- Der Hyperlink stimmt nicht mit der URL überein.
- Wenn ein Freund mir ein Foto zum Herunterladen schickt, besteht keine Gefahr, dies zu tun.
- Das Konto einer berühmten Marke muss von mir als vertrauenswürdig verifiziert werden.

Übung MULTIPLE CHOICE

Die Lage: Was sollten Sie tun, um zu garantieren, dass Sie Ihre Plattform für soziale Netzwerke sicher nutzen?

Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Es ist sicherer, dasselbe Passwort für alle meine Konten zu verwenden. Auf diese Weise werde ich es nie vergessen.
- Bevor ich die Anfrage eines neuen Freundes annehme, sollte ich die Authentizität seines Profils und seines Kontos überprüfen.



Co-funded by the
Erasmus+ Programme
of the European Union

- Ich sollte niemals Einzelheiten darüber preisgeben, wo ich Urlaub mache, einkaufe oder reise, und auch nicht, wann ich voraussichtlich abreisen oder nach Hause zurückkehren werde.
- Es ist in Ordnung, einen internetfähigen Computer zu betreiben, ohne Antimalware und Antiviren-Software zu installieren.
- Um alle sozialen Aktivitäten meiner Cyber-Freunde verfolgen zu können, muss ich jederzeit in mein Konto eingeloggt sein.



Quellen

Akilawala, T. (August 16, 2014) *Fake Robin Williams goodbye video on Facebook is a scam*. Retrieved from <https://www.bgr.in/news/fake-robin-williams-goodbye-video-on-facebook-is-a-scam-321750/>

Crowdstrike (October 15, 2019) *The 11 most common types of malware*. Retrieved from <https://www.crowdstrike.com/epp-101/types-of-malware/>

Constanza, T. (August 19, 2019) *Scam on Facebook exploits Robin Williams' suicide*. Retrieved from <https://www.siliconrepublic.com/enterprise/scam-on-facebook-exploits-robin-williams-suicide>

DuPaul, N. (October 12, 2012) *Common Malware Types: Cybersecurity 101*. Retrieved from <https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101>

Foreman, C. (June 20, 2017) *10 Types of Social Media and How Each Can Benefit Your Business*. Retrieved from <https://blog.hootsuite.com/types-of-social-media/>

Get Safe Online (n. d.) *Social Media Phishing*. <https://www.getsafeonline.org/social-networking/social-media-phishing/>

GMA News Online (August 15, 2014) *Beware of Robin Williams goodbye video scam*. Retrieved from <https://www.gmanetwork.com/news/hashtag/content/375009/beware-of-robin-williams-goodbye-video-scam/story/>

Kietzmann, J. H. and Hermkens, K. (2011) *Social media? Get serious! Understanding the functional building blocks of social media*. Business Horizons (Submitted manuscript). 54 (3): 241–251. doi:10.1016/j.bushor.2011.01.005.

Mohsin, M. (February 7, 2020) *10 Social Media Statistics You Need to Know in 2020 [Infographic]*. Retrieved from <https://www.oberlo.com/blog/social-media-marketing-statistics>

NortonLifeLock (n. d.) *What is a Trojan? Is it a virus or is it malware?* Retrieved from <https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html>

NortonLifeLock (n. d.) *What is a computer worm, and how does it work?* Retrieved from <https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html>

Obar, J. A. and Wildman, S. (2015) *Social media definition and the governance challenge: An introduction to the special issue*. Telecommunications Policy. 39 (9): 745–750. doi:10.1016/j.telpol.2015.07.014. SSRN 2647377

SNL. 2010. Saturday Night Live. Season 36, Episode 10. First aired December 18. NBC. Retrieved from https://www.youtube.com/watch?v=md3of7O02e4&list=PLS_gQd8UBhLghdS1aaLqVJ74rWi4fft8&index=14

Woodfield, M. (November 26, 2014) *Should I Buy from This Site? How to Know if a Website is Secure*. Retrieved from <https://www.digicert.com/blog/how-to-know-if-a-website-is-secure/>

ZeroFOX Alpha Team (February 15, 2017) *Social Media Impersonators Go Phishing: 3 Emerging Tactics*. <https://www.zerofox.com/blog/social-media-impersonators-phishing/>



Wissen sichern

Wir leben in einer Welt der Globalisierung, in der das Internet es uns ermöglicht, mit jedem überall auf der Welt zu kommunizieren. Social-Media-Plattformen sind zu einem **integralen Bestandteil unseres Lebens** geworden und bietet eine hervorragende Möglichkeit, mit anderen in Verbindung zu bleiben. Soziale Netzwerke wie Facebook, Instagram oder YouTube sind bei allen Altersgruppen beliebt und arbeiten ständig daran, Strömungen und neue NutzerInnen zu fesseln.

Trotz aller Vorteile, die diese Art von Plattformen für die NutzerInnen bieten, gibt es dennoch viele **Sicherheits- und Datenschutzrisiken**, die mit ihrer ständigen und unvorsichtigen Nutzung verbunden sind. Tatsächlich nutzen BetrügerInnen die Gewohnheiten der BenutzerInnen in den sozialen Medien aus, um sie zu **Phishing-Betrügereien und Angriffen** zu verleiten, die ihre Geräte und Daten kompromittieren. Daher sollte jeder seine Verantwortung für die Aufrechterhaltung **einer sicheren Online-Umgebung** anerkennen und gleichzeitig die Risiken einer Online-Präsenz verstehen. **Vorsicht, die Wahl eines starken Passworts oder die Installation von Antiviren-Software** sind einige von vielen Maßnahmen, die ein Nutzender ergreifen muss, um die Kontrolle über seine Sicherheit bei der Nutzung sozialer Netzwerke zu erlangen.

Da sich die Welt zu einem digitalen Binnenmarkt entwickelt, ist es von grundlegender Bedeutung, dass sich jeder über die Gesetze zum Schutz persönlicher Daten, wie z.B. das **GDPR**, im Klaren ist und weiß, wie diese für verschiedene digitale Szenarien gelten.

Zusammenfassend lässt sich sagen, **dass Regierung, Gesellschaft und EndbenutzerInnen zusammenarbeiten müssen, um die Privatsphäre und die Sicherheit von persönlichen Daten in sozialen Netzwerken zu schützen.**



Lösungsschlüssel

(die korrekten Antworten sind fett markiert)

1. Wissen anwenden

Situation: Was sind "Soziale Medien"?

Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Website und Anwendungen, die es Menschen ermöglichen, Nachrichten und Fotos zu versenden.
- Soziale Medien sind eine Form der elektronischen Kommunikation (z.B. Websites für soziale Netzwerke).
- Websites und Computerprogramme, die es Menschen ermöglichen, über das Internet mit Hilfe eines Computers oder Mobiltelefons zu kommunizieren und Informationen auszutauschen.
- Soziale Medien beziehen sich auf Websites und Anwendungen, die so gestaltet sind, dass Inhalte schnell ausgetauscht werden können.

Situation: Welche Rechte zum Schutz personenbezogener Daten werden in WhatsApp angewendet?

Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus: Nur eine Antwort ist falsch.

- Sie haben das Recht auf verschlüsselte Nachrichten, was bedeutet, dass WhatsApp die Nachrichten, die Sie an andere Personen senden, nicht lesen kann.
- Sie haben das Recht, Ihren WhatsApp-Account zu löschen, was bedeutet, dass die Nachrichten, die Sie an andere Personen gesendet haben, nicht mehr gelesen werden können.
- Wenn Sie nur die Anwendung WhatsApp auf Ihrem Gerät löschen, aber den Account nicht löschen, bleiben die Informationen erhalten.
- WhatsApp speichert und bewahrt Informationen über Sie auf, kann Ihre Informationen aber nicht überall auf der Welt verwenden.

2. Wissen anwenden

Situation: Welche Aussage ist falsch?

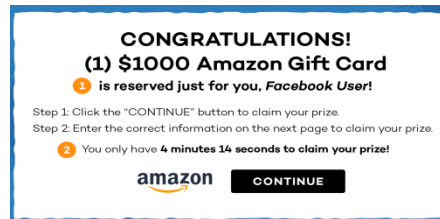
Aufgabe: Wählen Sie die richtige Option nach dem Single-Choice-Prinzip: Nur eine Option ist richtig.

- Soziale Medien sind ein wirksames Marketinginstrument für Unternehmen
- Facebook ist die meistgenutzte soziale Medienplattform
- Die meisten Nutzer sozialer Medien greifen über mobile Geräte auf soziale Kanäle zu
- Kleine und mittlere Unternehmen nutzen derzeit soziale Medien, um das Unternehmenswachstum voranzutreiben
- Die Benutzer neigen dazu, sich für ein soziales Netzwerk zu entscheiden und es täglich zu nutzen.

Situation: Sie scrollen durch Facebook und sehen die folgende Publikation:



Co-funded by the
Erasmus+ Programme
of the European Union



Was würden Sie tun?

Aufgabe: Wählen Sie die richtige Option nach dem Single-Choice-Prinzip aus: Nur eine Option ist richtig.

- OMG, heute ist mein Glückstag! Ich klicke auf "WEITER" und gebe ihnen alle notwendigen Daten, um die Geschenkkarte zu gewinnen. Danach teile ich die Gelegenheit mit all meinen Cyber-Freunden!
- Ich habe nur 4 Minuten, um meinen Preis einzufordern! Ich klicke auf "WEITER" und gebe ihnen alle notwendigen Daten, um den Preis zu gewinnen. Aber nachdem ich gesehen habe, dass ich Bankdaten angeben muss, gebe ich auf. Zu viel Arbeit.
- Ich werde neugierig und klicke auf "WEITER". Nachdem ich gesehen habe, dass es notwendig ist, ihnen persönliche Daten mitzuteilen, schließe ich die Registerkarte. Ich denke, es ist ein Betrug.
- **Ich klicke nicht in die Publikation. Ich kann keine Lotterie gewinnen, an der ich nie teilgenommen habe! Ich signalisiere den Beitrag an Facebook als "Betrug".**

3. Wissen anwenden

Situation: Was sind die Anzeichen für einen möglichen Phishing-Betrug, dass Sie beim Surfen in sozialen Medien immer wachsam sein müssen?

Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Grammatik und Rechtschreibung der Veröffentlichung.**
- Das Vorhandensein von Hyperlinks: Nur eine glaubwürdige Quelle kann einen Link zu ihrer Website veröffentlichen.
- **Der Hyperlink stimmt nicht mit der URL überein.**
- Wenn ein Freund mir ein Foto zum Herunterladen schickt, besteht keine Gefahr, dies zu tun.
- **Das Konto einer berühmten Marke muss von mir als vertrauenswürdig verifiziert werden.**

Die Lage: Was sollten Sie tun, um zu garantieren, dass Sie Ihre Plattform für soziale Netzwerke sicher nutzen?

Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Es ist sicherer, dasselbe Passwort für alle meine Konten zu verwenden. Auf diese Weise werde ich es nie vergessen.
- **Bevor ich die Anfrage eines neuen Freundes annehme, sollte ich die Authentizität seines Profils und seines Kontos überprüfen.**
- **Ich sollte niemals Einzelheiten darüber preisgeben, wo ich Urlaub mache, einkaufe oder reise, und auch nicht, wann ich voraussichtlich abreisen oder nach Hause zurückkehren werde.**
- Es ist in Ordnung, einen internetfähigen Computer zu betreiben, ohne Antimalware und Antiviren-Software zu installieren.
- Um alle sozialen Aktivitäten meiner Cyber-Freunde verfolgen zu können, muss ich jederzeit in mein Konto eingeloggt sein.