Lerneinheit

[Informationsfluss und Online-Kommunikation]

Projekt: B-SAFE
Nummer: 2018-1CZ01-KA204-048148

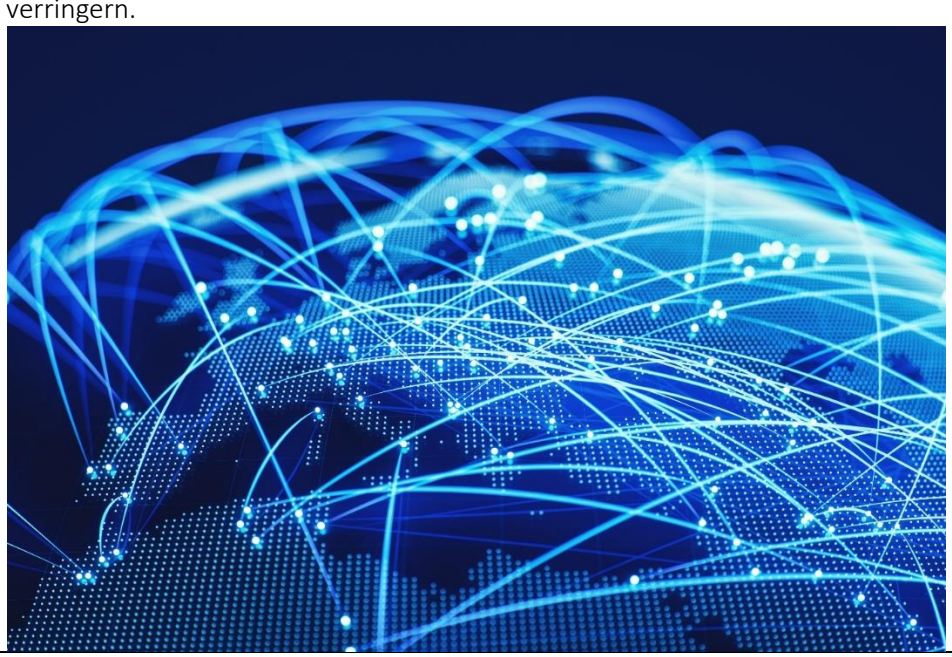
Funded by the Erasmus+ Programme of the European Union

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

Das Thema

Einführung

Das Internet hat die Art und Weise, wie wir miteinander kommunizieren, massiv beeinflusst. Für die meisten von uns gehört die Online-Kommunikation einfach zum Alltag. Unzählige E-Mails werden geöffnet, weitergeleitet und beantwortet. Auf diese Weise können Informationen schnell, einfach und kostengünstig weitergegeben werden. Irgendwie funktioniert Ihr E-Mail-Programm nicht richtig? Fangen wir mit dem Surfen im Internet an-es ist einfach, ein Forum zu finden, in dem jemand ähnliche Probleme beschreibt oder andere BenutzerInnen nützliche Tipps mit der Online-Community austauschen. Wie Sie sehen, gibt es keinen Zweifel, dass die Online-Kommunikation viele Vorteile bietet. Der alltägliche Gebrauch von E-Mails und anderen elektronischen Kommunikationsmitteln, der als selbstverständlich vorausgesetzt wird, verleitet jedoch dazu, unvorsichtig zu werden und damit potenzielle Risiken zu spät oder gar nicht zu erkennen. Umso wichtiger ist es zu wissen, worauf man bei der Nutzung der Online-Kommunikation wirklich achten sollte, um das Risiko negativer Folgen zu verringern.



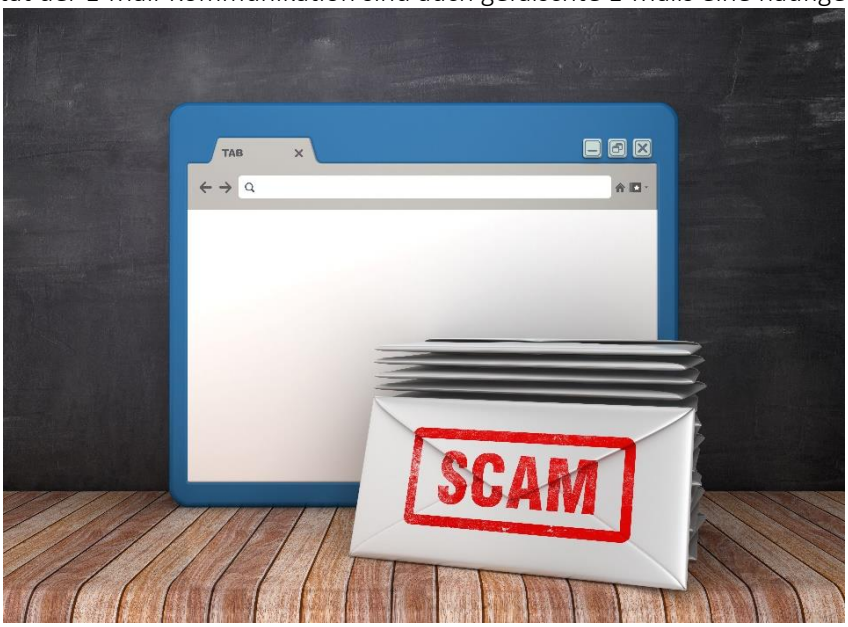
Praktische Relevanz - Hierfür benötigen Sie das Wissen und die Fähigkeiten

Die zunehmende Nutzung des Internets und verschiedener elektronischer Kommunikationsmittel - sowohl in unserem privaten als auch in unserem beruflichen Leben - schafft zusätzliche Bedrohungen für die Sicherheit unserer Daten und unserer Privatsphäre. Es ist deshalb wichtig, die aktuellen Datenschutzrisiken zu kennen, um sie schnell erkennen und gegebenenfalls richtig reagieren zu können. In Zeiten zunehmender Cyberkriminalität ist das entsprechende Know-how über mögliche Sicherheitsprobleme im Zuge der Online-Kommunikation sowie der korrekte und sichere Umgang mit E-Mails ein Muss für jeden Internet-Nutzer bzw. jede Internet-Nutzerin.

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

1.Wissen aufbauen – Gefälschte E-Mails und Anhänge

Das beliebteste Online-Kommunikationsmedium ist die E-Mail. Das Öffnen und Versenden von E-Mails gehört höchstwahrscheinlich auch zu Ihrer täglichen Routine, nicht wahr? Aber gerade wegen der hohen Popularität der E-Mail-Kommunikation sind auch gefälschte E-Mails eine häufige Bedrohung.



Definition
Gefälschte E-Mails sind unerwünschte E-Mails, die Sie bösgläubig mit betrügerischen Informationen in die Irre führen oder Sie zu schädlichen Handlungen verleiten. Beispielsweise werden bösartige Programme oft über Anhänge in gefälschte E-Mails **übertragen.**

Es ist daher wichtig, die typischen Merkmale bösartiger E-Mails zu kennen. Bevor Sie Anhänge öffnen, auf Links klicken oder E-Mails beantworten, kann es hilfreich sein**, sich die folgenden Fragen zu stellen**:

1. Wurde Ihnen etwas versprochen, von dem Sie glauben, **es sei zu schön, um wahr zu sein**? Seien Sie vorsichtig: Wenn es zu gut ist, um wahr zu sein, ist es ganz sicher nicht real.

Beispiel
Beispiele dafür sind in der Regel sehr attraktive Damen, die Sie kennen lernen möchten, Gratisgeschenke oder die Benachrichtigung, dass Sie einen Preis gewonnen haben (obwohl Sie an keinem Gewinnspiel teilgenommen haben).

2. Stimmt der Inhalt der E-Mail irgendwie **nicht mit dem (vermeintlich) vertrauenswürdigen E-Mail-Absender überein**?

Beispiel
Sie haben eine E-Mail von Ihrer Freundin Anna erhalten. Sie schreibt, dass sie im Ausland Urlaub macht und Opfer eines Diebstahls geworden ist. Anna bittet Sie deshalb dringend, sofort Geld auf ein Konto zu überweisen, damit sie das letzte Flugzeug in dieser Woche nach Hause nehmen kann. Solche Inhalte weisen eindeutig darauf hin, dass das E-Mail-Konto Ihrer Freundin Anna gehackt wurde.

3. Enthält die E-Mail als **Betreff bestimmte irritierende Wörter** wie „letzte Mahnung“, „Konto gesperrt“ oder ähnliches? Werden Sie aufgefordert, Ihre Zugangsdaten, Passwörter oder andere **vertrauliche Informationen** preiszugeben?

Wichtig
Wann immer jemand Sie drängt, sich zu beeilen oder vertrauliche Informationen preiszugeben, sollte er die Alarmglocken läuten lassen!

4. Erscheint Ihnen **der Absender fremd** (z.B. erhalten Sie eine englische Post von einer deutschen Firma)? Oder enthält die E-Mail viele **Rechtschreib- oder Grammatikfehler** (wahrscheinlich aufgrund von automatischen Übersetzungsprogrammen)?

5. Wurde die E-Mail automatisch in den **Spam-Ordner verschoben**?

Vielleicht fragen Sie sich jetzt, warum Sie überhaupt über Spam-E-Mails nachdenken sollten. Viele E-Mail-AnbieterInnen verbessern ständig ihre automatisierte Überwachung und deshalb landen unerwünschte E-Mails automatisch im sogenannten Spam-Ordner. Das Problem ist jedoch, dass es auch vorkommen kann, dass eine E-Mail fälschlicherweise als potenziell unerwünscht betrachtet wird und im Spam-Ordner landet.

Beispiel
Ihr Freund feiert eine große Party zu seinem Geburtstag. Er versendet die Einladungen per E-Mail an viele Eingeladene gleichzeitig, indem er alle E-Mail-Adressen unter BCC eingibt. Leider ist es möglich, dass Ihre Einladung im Spam landen wird, da viele Adressen im BCC ein typisches Zeichen für Spam-Mail sind.

6. Werden Sie aufgefordert, Programme mit seltsamen Dateinamen auszuführen (z.B. Kompositionen aus bekannten Dateinamen wie "jpg.vbs" oder "gif.exe")?

Wenn Sie auf eine oder mehrere dieser Fragen mit "Ja" antworten mussten oder wenn Ihnen eine Mail aus anderen Gründen verdächtig erscheint, sollten Sie die **Mail oder die darin enthaltenen Dateien und Links nicht öffnen**.

Sogenannte **Pishing-Mails** erfordern besondere Vorsicht.

Definition
Der Begriff **Phishing** setzt sich aus den beiden Wörtern "Passwort" und "Fischen" zusammen. Phishing ist der Versuch, an **fremde Passwörter** mit Hilfe von gefälschten E-Mails zu gelangen.

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

Vielleicht haben Sie bereits eine **seltsame E-Mail** von Ihrer Bank oder einem Ihnen bekannten Online-Shop erhalten. In vielen Fällen wird Ihnen mitgeteilt, dass Ihre Benutzerdaten leider verloren gegangen sind, dass Ihr Passwort abgelaufen ist oder dass aufgrund einer Aktualisierung dringend eine neue Identifikation erforderlich ist. Bequemerweise wird in der Regel direkt **ein Link auf die Website des Unternehmens** verschickt. Diese Websites sehen den Originalen **sehr ähnlich**, sind aber **gefälscht**. Wenn Sie Ihre Bankzugangsdaten in gutem Glauben eingeben, erhalten die BetrügerInnen Zugang dazu und können Ihnen Schaden zufügen.

Tipp
Mails, in denen Sie zur Bekanntgabe Ihrer Benutzerdaten aufgefordert werden, sollten niemals beantwortet werden. Seriöse Unternehmen würden dies nicht verlangen. Wenn Sie noch unsicher sind, ist es sinnvoll, den vermeintlichen Absender der Mail telefonisch zu befragen!

Darüber hinaus können die folgenden Maßnahmen dazu beitragen, **das Risiko** der Online-Kommunikation durch E-Mails zu **verringern**:

- Aktivieren Sie die Anzeige der Dateierweiterung (z.B. .docx, .exe). Dadurch können Sie Schadprogramme, die als E-Mail-Anhänge gesendet werden, besser identifizieren.
- Verwenden Sie geeignete Sicherheitseinstellungen, um die Ausführung von aktiven Inhalten in E-Mail-Programmen zu verhindern. So können Sie z.B. verhindern, dass beim Öffnen einer E-Mail unerwünschte Schadsoftware ausgeführt wird.
- Speichern Sie verdächtige Anhänge zuerst, damit Sie sie mit einem Virenprogramm überprüfen können.

1.Wissen anwenden

Übung MULTIPLE CHOICE

Situation: Was ist mit dem Begriff "gefälschte E-Mail" gemeint?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Gefälschte E-Mails sind unerwünschte E-Mails, die oft Malware enthalten, die als Anhang verschickt wird.

- Gefälschte E-Mails enthalten oft falsche oder unwahre Informationen.
- Es kann sein, dass gefälschte E-Mails vom angeblichen Absender gar nicht gesendet wurden.
- Gefälschte E-Mails sind E-Mails ohne jeglichen Inhalt. Diese leeren E-Mails wurden entweder absichtlich oder als versehentliche Nachricht versandt.

Übung MULTIPLE CHOICE

Situation: Sie überprüfen Ihr E-Mail-Konto und stellen viele neue E-Mails fest. In welchem der folgenden Fälle besteht eine hohe Wahrscheinlichkeit für eine gefälschte E-Mail?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Man verspricht Ihnen eine große Auszahlung
- - Sie werden dringend gebeten, Ihre Zugangsdaten zu ändern
- Die E-Mail hat keinen Betreff.
- - In der Betreffzeile steht: „letzte Mahnung“
- - Die E-Mail enthält eine auffällige Anzahl von Rechtschreibfehlern
- - Die E-Mail wurde automatisch in den Spam-Ordner verschoben
- - Die E-Mail wurde in den frühen Morgenstunden verschickt.

Übung MULTIPLE CHOICE

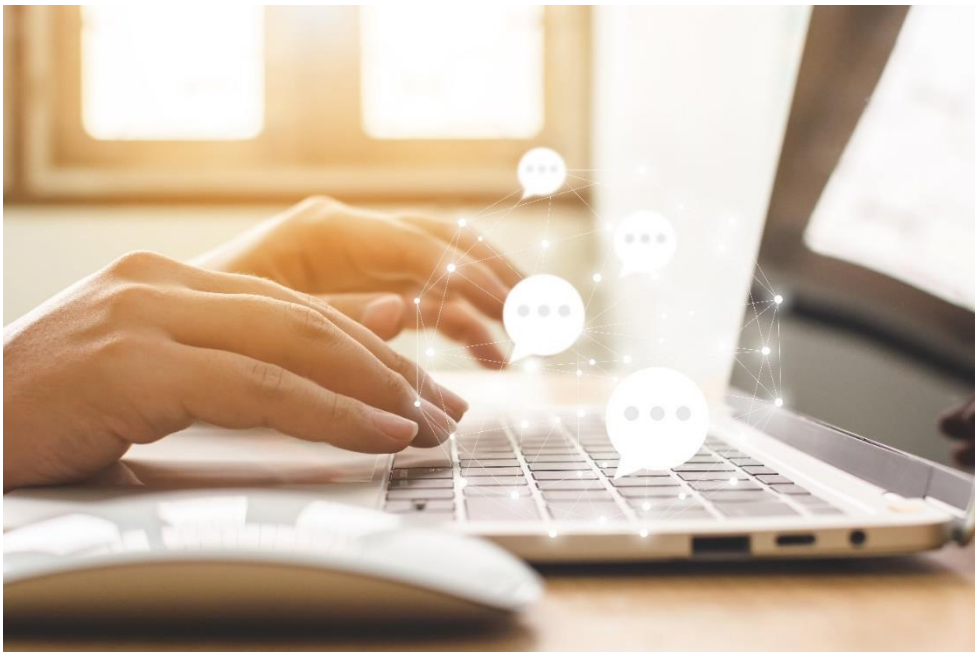
Situation: Welche Maßnahmen können Ihnen helfen, das Risiko der Online-Kommunikation über E-Mails zu reduzieren?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Aktivieren Sie die Anzeige der Dateierweiterung (z.B. .docx, .exe)
- Deaktivieren Sie die Anzeige der Dateierweiterung.
- Verhindern Sie durch geeignete Sicherheitseinstellungen die Ausführung aktiver Inhalte in E-Mail-Programmen
- Scannen Sie verdächtige Anhänge mit einem Virenprogramm
- Geben Sie Ihre Benutzerdaten nur dann weiter, wenn Sie die anfragenden Firmen sehr gut kennen

2.Wissen aufbauen - Foren und Chaträume

Foren und Chatrooms sind bekannte und beliebte Medien für die Online-Kommunikation und den Informationsaustausch, aber sie unterscheiden sich in der Art und Weise, wie sie genutzt werden.

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



Definition
Während sich Chat-Räume auf die Kommunikation mit Menschen **in Echtzeit** konzentrieren, eignen sich Foren eher für **Diskussionen, bei denen nicht alle TeilnehmerInnen gleichzeitig online sein müssen**. Foren sind in der Regel auch besser organisiert, wobei die Diskussionen in Threads unterteilt sind, die moderiert werden.

Chats und Foren ermöglichen den Austausch von Textnachrichten, können aber in der Regel auch zum Austausch von Bildern, Videos, Links oder Dateien genutzt werden. Zusätzlich unterstützen einige Chat-Räume auch die Verwendung von Mikrofonen oder Webcams zum Chatten mit anderen NutzerInnen.

Für die aktive Teilnahme an Foren und Chats ist in der Regel eine **Registrierung mit einer gültigen E-Mail-Adresse** erforderlich. Dies dient z.B. der Vermeidung von Spam-Posts. Darüber hinaus haben Moderatoren auch die Möglichkeit, NutzerInnen in Foren oder Chats zu suspendieren oder zu sperren, wenn sie sich unangemessen verhalten. Gleichwohl kann die Nutzung dieser Kommunikationsmedien verschiedene Risiken und Bedrohungen mit sich bringen, dazu gehören zum Beispiel:

- Maleware oder Links zu Phishing-Sites: Alle Dateien und Links, die in Foren veröffentlicht werden, sollten daher mit Vorsicht behandelt werden.
- Sie sollten bedenken, dass das Fälschen oder Hacken von Benutzerkonten Sie zur Annahme falscher Identitäten verleiten kann.
- Die Kommunikation in Foren und Chats erfolgt in der Regel völlig unverschlüsselt, so dass Ihre Aussagen und schriftlichen Informationen von allen NutzerInnen gelesen werden können. Auch für Fachleute ist es kein Problem, private Nachrichten zu lesen.

Sie wollen auf Foren und Chats nicht verzichten und fragen sich, was Sie tun können, um Sicherheitsrisiken zu vermeiden? Die Berücksichtigung der folgenden Aspekte ist sicherlich ein wichtiger Schritt:

- Öffnen Sie keine an Sie gesendeten Dateien, ohne diese kritisch zu hinterfragen.
- Geben Sie niemals persönliche und sensible Daten an Personen weiter, die Sie nicht persönlich kennen.
- **Erlauben Sie niemandem den Zugriff auf Ihren Computer**, auch nicht innerhalb einer Chat-Sitzung.

Beispiel
Sie haben ein Computerproblem und suchen Rat in einem ExperteInnen-Chat. Ein/e vermeintliche/r Experte/In will Ihnen helfen. Deshalb sollten Sie ihm/ ihr die Kontrolle über Ihren Computer per Fernsteuerung übertragen.

- Sie sollten die **Allgemeinen Geschäftsbedingungen und die Datenschutzbestimmungen des Kommunikationsdienstes lesen**, insbesondere im Hinblick darauf, was mit Ihren Daten und Informationen geschieht. Werden sie verkauft, gespeichert oder verschlüsselt?
- **Sperren Sie Kontakte**, wenn Sie sich nicht sicher sind, wer sie sind oder wenn Sie von jemandem belästigt werden. Melden Sie Beleidigungen, sexuelle Belästigung, Erpressung oder Drohungen bei der Polizei.
- Vergessen Sie nicht das **Urheberrecht:** Sie sollten keine Bilder oder andere Dateien, die Sie nicht selbst erstellt haben, ohne die Erlaubnis der AutorInnen versenden.
- Seien Sie immer **vorsichtig, wenn Sie mit einem Fremden ausgehen**, den Sie nur aus Foren oder Chats kennen. Selbst wenn Sie den Eindruck haben, dass Sie die Person bereits kennen, können die Informationen und Aussagen dieser Person allesamt gefälscht oder erfunden sein.

2. Wissen anwenden

Übung MULTIPLE CHOICE

Situation: Was sind Chatrooms und was verstehen Sie unter Foren? Wie unterscheiden sich die beiden Kommunikationsmittel voneinander?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Chatrooms eignen sich sehr gut für Diskussionen, bei denen nicht alle TeilnehmerInnen gleichzeitig online sein müssen.
- Foren eignen sich besser für Gespräche mit anderen in Echtzeit als Chat-Räume.
- Textnachrichten können sowohl in Chat-Räumen als auch in Foren ausgetauscht werden. Häufig können auch Bilder, Videos, Links oder Dateien ausgetauscht werden.
- Chat-Räume eignen sich besser für die Kommunikation mit anderen in Echtzeit als Foren.
- Während Sie in Chat-Räumen auch anonym oder unter einem Pseudonym chatten können, ist es notwendig, in Foren Ihren echten Namen preiszugeben.

Übung MULTIPLE CHOICE

Situation: Foren und Chatrooms sind sehr beliebte Online-Kommunikationsmittel. Welchen der folgenden Risiken können Sie jedoch bei ihrer Nutzung begegnen?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Die Infektion mit bösartiger Software durch das Öffnen von Dateien, die in Chatrooms oder Foren ausgetauscht werden.
- Die Umleitung zu Phising-Sites, indem man in gutem Glauben auf freigegebene Links klickt.
- Dass Ihnen durch den Austausch von Nachrichten in Foren plötzlich sehr hohe Kosten entstehen.
- Dass jemand versucht, Ihnen eine gefälschte oder erfundene Identität vorzutäuschen.

- Dass Ihre gesendeten Chat-Nachrichten heimlich auch von Dritten gelesen werden.

Übung MULTIPLE CHOICE

Situation: Welche der folgenden Maßnahmen können Sie ergreifen, um das Risiko der Online-Kommunikation über Foren und Chatrooms zu verringern?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Lesen Sie die allgemeinen Geschäftsbedingungen des Kommunikationsdienstes.
- Blockieren Sie Kontakte, wenn Sie sich nicht sicher sind, wer sie sind.
- Geben Sie nur Bilder oder Dateien weiter, die Sie nicht selbst entworfen haben.
- Erlauben Sie jemandem nur dann den Zugriff auf Ihren Computer, wenn er ein vertrauenswürdiges Profilfoto und einen Benutzernamen hat.
- Öffnen Sie keine an Sie gesendeten Dateien, ohne diese kritisch zu prüfen.

3. Wissen aufbauen - Kommunikation in sozialen Netzwerken

In sozialen Netzwerken kann die Annahme der vermeintlichen Anonymität zu **gedankenlosem Verhalten im Umgang mit Daten und Informationen** führen. Als Folge davon werden soziale Netzwerke zunehmend zur Zielscheibe betrügerischer Aktivitäten.

Im Umgang mit Social Media sollten Sie immer die **folgenden Aspekte berücksichtigen**:

- Veröffentlichen und diskutieren Sie niemals persönliche und vertrauliche Informationen im öffentlichen virtuellen Raum. Es kann rechtliche Konsequenzen haben, wenn Sie unüberlegte und unbeweisbare Behauptungen veröffentlichen.
- Jedes soziale Netzwerk hat die Möglichkeit, persönliche Informationen über Filter nur bestimmten Kategorien von Personengruppen zugänglich zu machen. Schauen Sie sich diese Optionen an, damit Sie nie Gefahr laufen, Tausende von Fremden zu Ihrer privaten Geburtstagsfeier begrüßen zu müssen.
- Sie möchten so viele Freunde wie möglich in sozialen Netzwerken haben? Achten Sie darauf, das gute alte Sprichwort nicht zu vergessen: "Zeig mir deine Freunde, und ich sage dir, wer du bist". **Freunde zu akzeptieren, ohne diese kritisch zu prüfen, kann sich negativ auf Sie auswirken** - z.B. wenn Sie auf der Suche nach einem Job sind. Viele ArbeitgeberInnen informieren sich in sozialen Netzwerken über die Aktivitäten der BewerberInnen und nutzen diese Informationen, um im Bewerbungsprozess Entscheidungen zu treffen.
- Prüfen Sie die Einstellungen in sozialen Netzwerken immer auf den Schutz der Privatsphäre.
- Seien Sie sich bewusst, dass gerade in sozialen Netzwerken die **Gefahr der Täuschung** besteht. Die Täter bzw. die Täterin täuschen und manipulieren ihre Opfer absichtlich, indem sie ihnen irreführende oder potenziell gefährliche Informationen zur Verfügung stellen.

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

Wichtig
Wenn Sie Missbrauch oder Fehlverhalten in sozialen Netzwerken feststellen, können und sollten Sie dies dem Anbieter und den zuständigen Behörden oder Organisationen melden.

3.Wissen anwenden

Übung MULTIPLE CHOICE

Situation: Was sollten Sie bei der Nutzung von Social Media beachten, um mögliche negative Folgen zu vermeiden?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Nehmen Sie so viele Freundschaftsanfragen wie möglich an, um sich bei anderen so beliebt wie möglich zu machen.
- Überprüfen Sie immer die Einstellungen für soziale Medien zum Schutz der Privatsphäre.
- Glauben Sie nicht allen Informationen, die Sie in sozialen Netzwerken erhalten.
- Wenn Sie jemanden nicht mögen und deshalb sehr negative Kommentare über ihn oder sie veröffentlichen möchten, achten Sie darauf, nicht Ihren wirklichen Namen zu verwenden, besonders wenn Sie eine harte Sprache verwenden. Auf diese Weise können Sie anonym bleiben und müssen keine Konsequenzen befürchten.

Übung MULTIPLE CHOICE

Situation: Sie überprüfen Ihr Social Media-Konto. Unter Schock stellen Sie fest, dass jemand ein Video ins Netz gestellt hat, das eine Gruppe Jugendlicher zeigt, die ein Mädchen wild schikaniert und misshandelt, sowohl physisch als auch psychisch. Wie sollten Sie jetzt reagieren?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Sie sollten es dem Dienstanbieter (z.B. Facebook) melden.
- Leider können Sie nichts tun. Vielleicht ist das Video nicht einmal echt. Um nicht selbst bedroht zu werden, ignorieren Sie es.
- Sie sollten es bei der Polizei melden.
- Sie kennen weder das Opfer noch den Täter bzw. die Täterin, also können Sie niemandem einen konkreten Namen nennen. Deshalb macht es keinen Sinn, dass Sie sich einmischen.

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

Quellen

wko.at: https://www.wko.at/site/it-safe/mitarbeiter-handbuch.pdf

klicksafe.de: https://www.klicksafe.de/themen/kommunizieren/chat/

onlinesicherheit.gv.at: https://www.onlinesicherheit.gv.at/gefahren_im_netz/soziale_medien/gefahren/250080.html

securitymetrics.com: https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

ftc.gov: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

smallbusiness.com: https://smallbusiness.chron.com/differences-between-chat-rooms-forums-71296.html

socialnomics.net: https://socialnomics.net/2017/11/08/chatting-online-risks-the-tips-to-stay-safe/

getsafeonline.org: https://www.getsafeonline.org/social-networking/chatrooms/

cybersecurity.edu: https://cybersecurity.osu.edu/cybersecurity-you/develop-safe-habits/social-media

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

Wissen sichern

Zusammenfassung

Die beliebteste Form der Online-Kommunikation ist die **E-Mail**, weshalb **gefälschte E-Mails** leider auch recht häufig vorkommen. Fake-E-Mails sind unerwünschte E-Mails mit böswillig falschen oder irreführenden Informationen. In den Anhängen dieser gefälschten E-Mails ist beispielsweise oft Malware versteckt.

Um nicht auf diese gefälschten E-Mails hereinzufallen, ist es wichtig, **wachsam zu bleiben**. Beispielsweise sollten E-Mails, die Ihnen einen großen Gewinn versprechen oder Sie zur Preisgabe vertraulicher Informationen auffordern, stets mit Vorsicht behandelt werden. Dasselbe gilt für E-Mails mit irritierenden Wörtern als Betreff wie "Ihr Bankkonto wurde gesperrt" oder mit einer ungewöhnlich hohen Anzahl von Grammatik- oder Rechtschreibfehlern.
Besondere Vorsicht ist bei sogenannten **Pishing-Mails** geboten, bei denen mit gefälschten E-Mails versucht wird, an Passwörter zu gelangen. Um das Risiko der Online-Kommunikation zu verringern, ist es sinnvoll, verdächtige E-Mail-Anhänge zunächst zu speichern und mit einem **Virenprogramm zu scannen**.

Es besteht auch die Gefahr, den Computer mit Malware zu infizieren oder bei **der Kommunikation in Foren oder Chatrooms** durch unachtsames Anklicken von Links oder Öffnen von Dateien auf Pishing-Seiten weitergeleitet zu werden. Falsche Identitäten oder ungewolltes Mitlesen von Nachrichten sind weitere Gefahren, die berücksichtigt werden müssen.
Es ist daher besonders wichtig, die **Datenschutzbestimmungen der Anbieter von Online-Kommunikation sorgfältig zu lesen** und **niemals persönliche oder sensible Daten** in Chats oder Foren preiszugeben.

Dies gilt auch bei **der Nutzung sozialer Netzwerke**. Seien Sie sich bewusst, dass gerade in sozialen Netzwerken die Gefahr besteht, durch falsche Identitäten oder durch die bewusste oder unbewusste Verbreitung **falscher Informationen** in die Irre geführt zu werden. Wenn Sie Missbrauch oder Fehlverhalten in sozialen Netzwerken feststellen, **können und sollten Sie** dies dem Dienstanbieter und den zuständigen Behörden oder Organisationen **melden**.

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

Lösungsschlüssel
(die korrekten Antworten sind fett markiert)

1.Wissen anwenden

Situation: Was ist mit dem Begriff "gefälschte E-Mail" gemeint?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Gefälschte E-Mails sind unerwünschte E-Mails, die oft Malware enthalten, die als Anhang verschickt wird.**
- **Gefälschte E-Mails enthalten oft falsche oder unwahre Informationen.**
- **Es kann sein, dass gefälschte E-Mails vom angeblichen Absender gar nicht gesendet wurden.**
- Gefälschte E-Mails sind E-Mails ohne jeglichen Inhalt. Diese leeren E-Mails wurden entweder absichtlich oder als versehentliche Nachricht versandt.

Situation: Sie überprüfen Ihr E-Mail-Konto und stellen viele neue E-Mails fest. In welchem der folgenden Fälle besteht eine hohe Wahrscheinlichkeit für eine gefälschte E-Mail?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Man verspricht Ihnen eine große Auszahlung**
- **- Sie werden dringend gebeten, Ihre Zugangsdaten zu ändern**
- Die E-Mail hat keinen Betreff.
- **- In der Betreffzeile steht: „letzte Mahnung“**
- **- Die E-Mail enthält eine auffällige Anzahl von Rechtschreibfehlern**
- **- Die E-Mail wurde automatisch in den Spam-Ordner verschoben**
- - Die E-Mail wurde in den frühen Morgenstunden verschickt.

Situation: Welche Maßnahmen können Ihnen helfen, das Risiko der Online-Kommunikation über E-Mails zu reduzieren?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Aktivieren Sie die Anzeige der Dateierweiterung (z.B. .docx, .exe)**
- Deaktivieren Sie die Anzeige der Dateierweiterung.
- **Verhindern Sie durch geeignete Sicherheitseinstellungen die Ausführung aktiver Inhalte in E-Mail-Programmen**
- **Scannen Sie verdächtige Anhänge mit einem Virenprogramm**
- Geben Sie Ihre Benutzerdaten nur dann weiter, wenn Sie die anfragenden Firmen sehr gut kennen

2.Wissen anwenden

Situation: Was sind Chatrooms und was verstehen Sie unter Foren? Wie unterscheiden sich die beiden Kommunikationsmittel voneinander?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Chatrooms eignen sich sehr gut für Diskussionen, bei denen nicht alle TeilnehmerInnen gleichzeitig online sein müssen.
- Foren eignen sich besser für Gespräche mit anderen in Echtzeit als Chat-Räume.

- Textnachrichten können sowohl in Chat-Räumen als auch in Foren ausgetauscht werden. Häufig können auch Bilder, Videos, Links oder Dateien ausgetauscht werden.
- Chat-Räume eignen sich besser für die Kommunikation mit anderen in Echtzeit als Foren.
- Während Sie in Chat-Räumen auch anonym oder unter einem Pseudonym chatten können, ist es notwendig, in Foren Ihren echten Namen preiszugeben.

Situation: Foren und Chatrooms sind sehr beliebte Online-Kommunikationsmittel. Welchen der folgenden Risiken können Sie jedoch bei ihrer Nutzung begegnen?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Die Infektion mit bösartiger Software durch das Öffnen von Dateien, die in Chatrooms oder Foren ausgetauscht werden.
- Die Umleitung zu Phising-Sites, indem man in gutem Glauben auf freigegebene Links klickt.
- Dass Ihnen durch den Austausch von Nachrichten in Foren plötzlich sehr hohe Kosten entstehen.
- Dass jemand versucht, Ihnen eine gefälschte oder erfundene Identität vorzutäuschen.
- Dass Ihre gesendeten Chat-Nachrichten heimlich auch von Dritten gelesen werden.

Situation: Welche der folgenden Maßnahmen können Sie ergreifen, um das Risiko der Online-Kommunikation über Foren und Chatrooms zu verringern?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Lesen Sie die allgemeinen Geschäftsbedingungen des Kommunikationsdienstes.
- Blockieren Sie Kontakte, wenn Sie sich nicht sicher sind, wer sie sind.
- Geben Sie nur Bilder oder Dateien weiter, die Sie nicht selbst entworfen haben.
- Erlauben Sie jemandem nur dann den Zugriff auf Ihren Computer, wenn er ein vertrauenswürdiges Profilfoto und einen Benutzernamen hat.
- Öffnen Sie keine an Sie gesendeten Dateien, ohne diese kritisch zu prüfen.

3.Wissen anwenden

Situation: Was sollten Sie bei der Nutzung von Social Media beachten, um mögliche negative Folgen zu vermeiden?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Nehmen Sie so viele Freundschaftsanfragen wie möglich an, um sich bei anderen so beliebt wie möglich zu machen.
- Überprüfen Sie immer die Einstellungen für soziale Medien zum Schutz der Privatsphäre.
- Glauben Sie nicht allen Informationen, die Sie in sozialen Netzwerken erhalten.
- Wenn Sie jemanden nicht mögen und deshalb sehr negative Kommentare über ihn oder sie veröffentlichen möchten, achten Sie darauf, nicht Ihren wirklichen Namen zu verwenden, besonders wenn Sie eine harte Sprache verwenden. Auf diese Weise können Sie anonym bleiben und müssen keine Konsequenzen befürchten.

Situation: Sie überprüfen Ihr Social Media-Konto. Unter Schock stellen Sie fest, dass jemand ein Video ins Netz gestellt hat, das eine Gruppe Jugendlicher zeigt, die ein Mädchen wild schikaniert und misshandelt, sowohl physisch als auch psychisch. Wie sollten Sie jetzt reagieren?

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

- Sie sollten es dem Dienstanbieter (z.B. Facebook) melden.
- Leider können Sie nichts tun. Vielleicht ist das Video nicht einmal echt. Um nicht selbst bedroht zu werden, ignorieren Sie es.
- Sie sollten es bei der Polizei melden.
- Sie kennen weder das Opfer noch den Täter bzw. die Täterin, also können Sie niemandem einen konkreten Namen nennen. Deshalb macht es keinen Sinn, dass Sie sich einmischen.