Kompetenzbereich 4: Sicherheit

Stolpersteine im Netz erkennen

In diesem Dokument zum Modul des Kompetenzbereichs 4 erfahren Sie mehr zum Thema „Sicherheit“ und welche Stolpersteine im Netz lauern können.

Was? Klingt langweilig? – Nicht für Claudia. Die hat nämlich pünktlich zum Feierabend ein E-Mail mit einem vielversprechenden Betreff bekommen: Ein Gewinn von 10.000 Euro soll auf sie warten. Aber wird sie dieses E-Mail wirklich öffnen? Erfahren Sie mehr dazu in diesem Dokument!

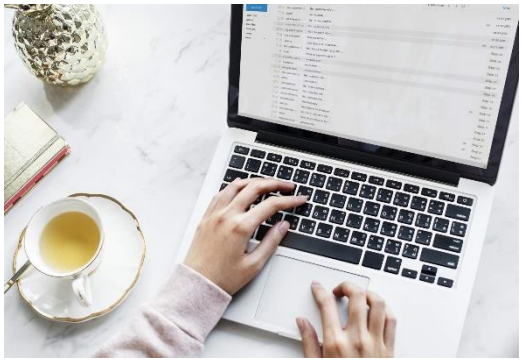
Einen Überblick über alle Infomodule zu den sechs Kompetenzbereichen des **Digitalen Kompetenzmodells für Österreich** finden Sie **hier**.

Themenübersicht

BETRUG IM NETZ

Möchten Sie mehr über den angeblichen Gewinn von Claudia erfahren?
Schauen Sie doch hier ins Online-Modul: https://www.fit4internet.at/→VERSTEHEN

Claudia öffnet das E-Mail und sieht, dass sie ihre Bankdaten bekanntgeben muss, um den Gewinn zu erhalten. Der beigefügte Link öffnet gleich ein neues Fenster, in dem sie ihre Daten eintragen soll. Die Vorfreude verfliegt und Claudia hat ein mulmiges Gefühl bei der Weitergabe ihrer Daten.



Oft versuchen Betrüger und Betrügerinnen im Netz mittels **gefälschter Websites** und E-Mails an die **Passwörter und Daten** ahnungsloser Personen für Online-Bankkonten, Online-Shops oder Ähnliches zu kommen.

Es wird eine **täuschend echte E-Mail** an die Person gesendet, in der sie aufgefordert wird, auf einen Link zu klicken, um sich in das Benutzerkonto einzuloggen. Die gesamte Website, auf die der Link verweist, ist allerdings ebenfalls gefälscht – auch wenn sie auf den ersten Blick exakt wie das Original aussieht.

Seien Sie **vorsichtig mit der Weitergabe von Benutzerdaten** und prüfen Sie zuerst genau, ob es sich um die echte Website oder eine Fälschung handelt. Banken fragen z. B. sensible Daten **niemals** unaufgefordert per E-Mail ab. Ignorieren Sie daher diese Nachrichten! Fragen Sie bei Unklarheit am besten telefonisch bei Ihrer Bank nach.

UNSERIÖSE WEBSITES ERKENNEN

Claudia sieht sich die Website genauer an und findet zahlreiche Fehler im Text. Die Navigation ist unübersichtlich und bei genauerer Suche findet sie das Impressum mit Firmensitz im Ausland, aber keine Allgemeinen Geschäftsbedingungen. Die Website sieht äußerst unseriös aus!

Unseriöse Websites lassen sich unter anderem an den folgenden Punkten erkennen:

- Es wird zur Teilnahme an Gewinnspielen aufgefordert.
- Das Impressum ist unvollständig (zum Beispiel ohne Angabe von Steuernummer oder Gesellschaftsform) oder nicht vorhanden.
- Es gibt keine Möglichkeit des Kontaktes.
- Der Firmensitz befindet sich im Ausland.
- Es gibt keine Datenschutzerklärung.

Wie kann man **Phishing vermeiden**?

- Nicht auf Links in ungebetenen E-Mails klicken.
- Keine Anhänge aus unerwarteten oder unbekannten E-Mails öffnen.
- Das Passwort schützen und niemandem mitteilen.
- Geben Sie niemandem sensible Informationen weiter – weder telefonisch, noch persönlich oder per E-Mail.
- Installieren Sie neue Updates für Ihren Browser, um ihn aktuell zu halten.

Was sind Phishing Mails?

Eine besondere Form des Online-Betruges ist „Phishing“ (vom englischen Wort „fishing“ abgeleitet). Hier versuchen Kriminelle auf betrügerische Art und Weise an Passwörter, Nummern von Kreditkarten, Sozialversicherungen oder Bankkonten zu gelangen. Sie versenden gefälschte E-Mails oder leiten ahnungslose Personen auf gefälschte Websites um.

Was ist Spam?

Als Spam bezeichnet man unerwünschte Nachrichten, die für eine Dienstleistung oder ein Produkt werben. Es ist quasi die elektronische Version von Werbesendungen. Vermeiden Sie, darauf zu antworten und verschieben Sie diese Nachrichten am besten direkt in den Papierkorb.

Was sind AGB?

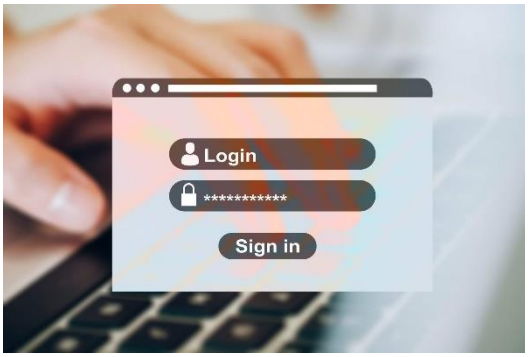
Bei den **Allgemeinen Geschäftsbedingungen (AGB)** handelt es sich um eine Zusammenfassung der Datenschutzbestimmungen des Online-Anbieters.

SICHERHEIT BEI ONLINE-GELDGESCHÄFTEN BEACHTEN

Claudia schließt die Website und löscht das E-Mail. Ihre Bank bietet zwar E-Banking an, aber der Link im E-Mail sah eindeutig nicht vertrauenswürdig aus.

Sicheres E-Banking erfordert eine Überprüfung der Identifikation, zum Beispiel in Form eines PIN-Codes, einer Verfügernummer und Passwort oder Fingerprint am Smartphone. Dies kann je nach Bankinstitut variieren.

Rufen Sie die Website der Bank durch Eintippen der Internetadresse im Browser auf. So verhindern Sie, dass Sie **irrtümlich** gefälschten Links folgen.



Sichere Passwörter bestehen aus einer **Kombination aus mindestens 8 Buchstaben** inklusive **Zahlen** und **Sonderzeichen**. Alternativ können Sie sich auch einen Satz überlegen und die Anfangsbuchstaben der Wörter als Passwort verwenden (z. B. Ich fahre täglich um 8 Uhr zur Arbeit – Iftu8UzA).

Wählen Sie stets verschiedene Passwörter für die Anwendungen, die Sie nutzen, und ändern Sie diese regelmäßig! Eine weitere Möglichkeit ist die Verwendung eines **Passwort-Managers**.

Was ist E-Banking?

Mit E-Banking können Bankgeschäfte einfach und bequem rund um die Uhr im Internet über PCs, Smartphones oder Tablets abgewickelt werden.

DAS SMARTPHONE SICHER NUTZEN

Claudia vermeidet grundsätzlich E-Banking in fremden oder öffentlichen WLAN-Netzen, da diese oft nicht ausreichend gesichert sind. Nur zuhause fühlt sie sich absolut sicher. Auch beim E-Banking über das Smartphone ist sie skeptisch. Ist das wirklich sicher?

Die meisten großen Banken bieten Smartphone-Programme (Apps) für E-Banking an. Einerseits ist es sicherer über die App einzusteigen, da so die Gefahr, auf eine gefälschte Seite zu gelangen, umgangen werden kann. Aber natürlich besteht wie bei jeder anderen App auch die Gefahr, dass diese gehackt wird oder das Smartphone von Viren befallen wird.

Was ist „Hacking“?

Personen (mitunter mit kriminellen Absichten) versuchen sich per „Hacking“ Zugang zu Systemen zum Beispiel PCs, Smartphones oder Software zu verschaffen und diese zu verändern oder zu manipulieren.

Was ist ein (Computer)-Virus?

Ein Computer-Virus ist ein Programm, das ohne Ihr Wissen oder Zustimmung auf Ihrem Gerät wie PC, Tablet oder Smartphone geladen wird. Manche Viren stören einfach nur, aber andere sind zerstörerisch und übernehmen die Kontrolle von Programmen und Systemen. Mittels diversen Virenschutz-Programmen (zum Beispiel Avira, Kaspersky, TOTALAV) kann man vorbeugend das Gerät schützen.

BEI SMARTPHONEVERLUST ODER -DIEBSTAHL RICHTIG HANDELN

Einmal beim Sport hat Claudia ihr Smartphone liegen lassen. Als sie es bemerkt hat, ist sie sofort mit Herzklopfen von zu Hause zurück ins Fitnessstudio gelaufen. Schweißgebadet ist sie dort angekommen und hat beim Empfang nachgefragt. Zum Glück wurde das Gerät von einem ehrlichen Finder abgegeben. Puh, das ist noch einmal gut gegangen. Aber was, wenn sie es nicht wiederbekommen hätte? Was ist bei Verlust oder Diebstahl zu tun und wie kann sie ihr Smartphone schützen?

Nach Verlust oder Diebstahl des Smartphones ist es möglich, die **SIM-Karte des Smartphones sperren** zu lassen. Kontaktieren Sie den Netzbetreiber und halten Sie Ihr Kundenkennwort bereit.
Das Sperren der SIM-Karte vermeidet einen Missbrauch der enthaltenen Freieinheiten, jedoch wird Datendiebstahl nicht verhindert!

> Schützen Sie den Zugang zu Ihrem Smartphone mit einem **Passwort, Zahlencode oder Fingerabdruck**, um im Verlustfall einem Datendiebstahl vorzubeugen.

Bei einem Diebstahl empfiehlt sich auch die **Erstattung einer Anzeige**. Für diese benötigen Sie die die **15-stellige Seriennummer** (IMEI-Nummer) des Smartphones. Mit der Anzeige ist die Sperre beim Netzbetreiber meistens kostenlos. Die IMEI-Nummer ist auf dem aufgeklebten Barcodeetikett auf der Verpackung des Geräts zu finden. Alternativ können Sie die Nummer auch durch die Eingabe von *#06# auf Ihrem Gerät abrufen (am besten Sie notieren sich diese Nummer nach Kauf des Geräts, um sie im Bedarfsfall zur Hand zu haben).

> Bei Verlust empfiehlt sich, zu versuchen, das Smartphone zu orten. Viele Smartphones haben einen **Ortungsdienst vorinstalliert**.

EINE ALTERSGERECHTE INTERNETNUTZUNG GEWÄHRLEISTEN

Claudia denkt an ihre Kinder, die bereits beide ein Smartphone besitzen und fast täglich den Computer und das Internet nutzen. Sie fragt sich, wie sie diese eigentlich vor Betrug im Internet, Phishing, nicht altersgerechten Inhalten und gesundheitlichen Risiken schützen kann.

Wichtig ist, dass Kinder schon früh lernen, das **Internet richtig** und vor allem auch **kritisch zu nutzen**. Nur so können sie von den vielen Chancen – die im Vergleich zu den Risiken deutlich überwiegen – profitieren.

> Was soll/darf mein Kind ab welchem Alter im Internet tun? Auf der Website von „saferinternet“ finden Sie weitere **Infos zur altersgerechten Internetnutzung**.

GESUNDHEITLICHE RISIKEN KENNEN

Ihre jüngste Tochter Hannah bereitet Claudia in letzter Zeit besonders Sorgen. Sie wirkt oft betrübt, trifft sich kaum mehr mit Freunden und verschließt sich immer mehr vor ihr. Was könnte hinter Hannahs verändertem Verhalten stecken?

Im Internet werden Kinder oft zur Zielscheibe für **Cyber-Mobbing** oder Belästigung. Die mögliche Anonymität, die das Internet bietet, lässt die Hemmschwelle für derartige Taten häufig sinken. Mobbing kann auch über SMS und Messenger am Smartphone auftreten.

Sollte man von anderen Personen im Internet belästigt werden, so kann man in der Regel über das eigene Profil oder Einstellungen unerwünschte Personen blockieren oder ignorieren. Diese können dann in der Regel nicht mehr auf das Ihr Profil zugreifen und auch keine Nachrichten mehr senden.

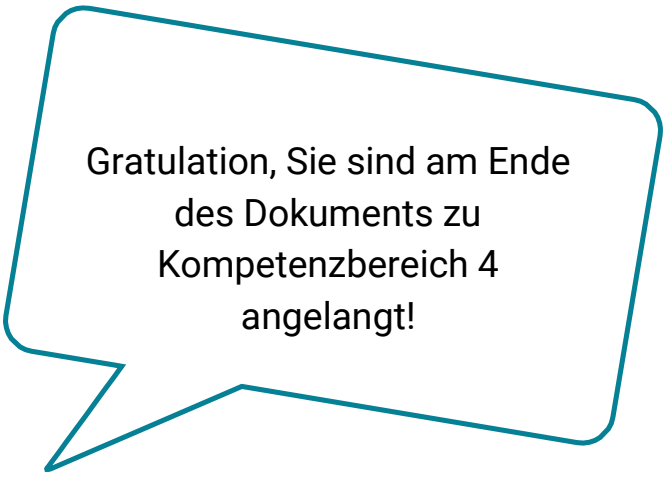
Nur sehr **wenige Menschen**, die viel Zeit am PC, Tablet oder Smartphone verbringen (zum Beispiel mit Online-Spielen), sind auch **wirklich krankhaft süchtig**. Dennoch kann eine ständige Verwendung des Smartphones zu Konzentrationsschwächen, Zerstreutheit, sozialem Stress und Angst führen. Wichtig ist: Nicht die reine Nutzungsdauer steht im Vordergrund, sondern vor allem die **Kontrolle über das eigene Verhalten** und die Möglichkeit, das Smartphone auch mal guten Gefühls beiseitelegen zu können.

Einige Smartphone-Modelle zeigen die tägliche **persönliche Bildschirmzeit** sowie einen Wochenüberblick aller App-Nutzungszeiten. Diese Übersicht kann helfen, sich seines Smartphone-Konsums besser bewusst zu werden.

Was ist Cyber-Mobbing?

Cyber-Mobbing bezeichnet das absichtliche und über längeren Zeitraum anhaltende Beleidigen, Bedrohen, Bloßstellen, Belästigen oder Ausgrenzen anderer Menschen über digitale Medien.

ABSCHLUSS UND AUSBLICK



Werfen wir noch einmal einen kurzen Blick zurück, was alles in diesem Modul passiert ist ...

Claudia weiß jetzt, dass sie leider keine 10.000 Euro gewonnen hat. Dafür hat sie gelernt, wie sie sich und ihre Kinder besser vor den Risiken des Internets schützen kann, um die ganzen Vorteile weiterhin entspannt genießen zu können. Und Sie wissen jetzt, was Phishing, Spam und Hacking bedeuten und wie Sie am besten mit diesen Gefahren umgehen. Ein guter alter Lottoschein ist dann wahrscheinlich doch die bessere Option als auf einen Link einer fremden E-Mail zu klicken …

Im nächsten Kompetenzbereich wird es dann um Problemlösen und Weiterlernen gehen. Mirko muss nämlich seine Lohnsteuer machen und lernt dabei, dass er nicht nur die Steuer, sondern auch noch viele weitere Dinge problemlos online erledigen kann.

IMPRESSUM

Medieninhaber
"fit4internet" - Verein zur Steigerung der digitalen Kompetenzen in Österreich
ZVR: 1882525812
c/o weXelerate
Praterstraße 1/ 1. OG/ Space 15
1020 Wien
ZVR-Zahl: 1882525812
office@fit4internet.at
MMag. Peter Oswald (Präsident), Mag.ª Ulrike Fiona Domany-Funtan, MBA (Generalsekretärin)

Inhalte und didaktische Umsetzung
common sense - eLearning & training consultants
Köllnerhofgasse 2/8
1010 Wien | Österreich
eMail: office@common-sense.at
Web: www.common-sense.at