MAKING SOCIAL CARE TECHNOLOGIES ACCESSIBLE TO ALL

Topic 1.3. Grundlagen der Online- und Cybersicherheit

Finanziert von der Europäischen Union. Die geäußerten Ansichten und Meinungen sind jedoch ausschließlich die des Autors/der Autorin und spiegeln nicht unbedingt die der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die EACEA können für diese verantwortlich gemacht werden.

Inhalt

Einführung

1. Überblick
2. Zielgruppe
3. Ausbildungsziele

Co-funded by the European Union

Einführung

1. Überblick

Worum geht es in diesem Training?

Das Curriculum "Grundlagen der Online- und Cybersicherheit" soll Beschäftigten im Pflegesektor wichtige Kenntnisse und Fähigkeiten zum **Schutz sensibler Daten und zur Gewährleistung der Online-Sicherheit** im Rahmen ihrer Arbeit vermitteln. Die Teilnehmenden lernen, wie sie gängige Cybersicherheitsrisiken **erkennen** und **mindern können** und wie sie **bewährte Verfahren** und einfach umzusetzende Maßnahmen für die Online-Sicherheit anwenden können.

Warum ist das notwendig?

Die transnationale Erhebung des SociALL-Projekts hat gezeigt: Cybersicherheit ist ein besonders **wichtiges und aktuelles** Thema in einem Kontext erhöhter Cybersicherheitsrisiken und der Sorge um den Schutz und die Integrität von Gesundheits- und personenbezogenen Daten. Die Zunahme von Cyberangriffen auf **gefährdete** Gesundheitseinrichtungen, wie die jüngsten Ransomware-Angriffe auf europäische Krankenhäuser zeigen, erfordert mehr Aufmerksamkeit und Wissen.

Co-funded by the European Union

Einführung

2. Zielgruppe

Für wen ist dieses Training?

Praktisch **jede Fachkraft, die im Pflegesektor arbeitet**, kann diesen Kurs besuchen, da nahezu alle täglich mit digitalen Werkzeugen arbeitet und somit Cyberrisiken ausgesetzt ist. Das Training besteht hauptsächlich aus Erklärungen, Tipps und bewährten Praktiken, die von den meisten individuell und ohne wichtige technische Kenntnisse angewendet werden können. Die meisten dieser Inhalte können den Arbeitnehmer:innen in ihrem Berufsleben hilfreich sein, aber sie auch in ihrer persönlichen Nutzung digitaler Werkzeuge unterstützen.

Was sind die Voraussetzungen?

Dieses Curriculum ist für **viele Beschäftigen im Pflegebereich** geeignet und bietet eine grundlegende, nützliche Einführung und Anleitung zu Cyber- und Online-Sicherheit. Jede Person, die es gewohnt ist, digitale Werkzeuge in ihrem Berufsleben zu nutzen, ist daher in der Lage, diesem Kurs zu folgen, ihn zu verstehen und daraus zu lernen.

Co-funded by the European Union

Einführung

3. Ausbildungsziele

Was kann mit diesem Training erreicht werden?

- Verständnis für die Bedeutung von Cybersicherheit und Online-Sicherheit.
- Verstehen der Risiken und häufigsten Bedrohungen
- Den menschlichen Faktor bei Cyberangriffen verstehen
- Anwendung einfach umzusetzender Maßnahmen für Datenschutz und Online-Sicherheit
- Nutzung nützlicher Ressourcen, Tools und weltweit anerkannter bewährter Verfahren zur Erhöhung der Sicherheit

Was wird sich ändern?

Am Ende des Trainings werden die Teilnehmenden und ihre Organisationen in der Lage sein, besser zu arbeiten:

- **Verankerung der** Online-Sicherheit in ihrem Betrieb
- **Identifizierung** und **Bewältigung von Cyber-sicherheitsrisiken**
- **Prozesse**, die sie **angreifbar** machen, durch sicherere Prozesse ersetzen
- Kolleg:innen **zu schulen und zu beraten**, um eine **sicherere Unternehmenskultur zu** schaffen
- Dieses Wissen an **Patient:innen weitergeben**, wenn die Pflegekräfte **Risiken** wahrnehmen

Co-funded by the European Union

1. Grundlagen Cyber- und Online-Sicherheit

1. Bedeutung von Cyber- und Online-Sicherheit
2. Verständnis von Pflegekräften für ihre Verantwortung in Bezug auf sensible Patient:innendaten
3. Menschliche Fehler und Nachlässigkeit sind das Haupteinfallstor für Cyber-Kriminalität
4. Was können wir tun?
5. Menschliche Schwachstellen erkennen und behandeln

1. Grundlagen Cyber- und Online-Sicherheit

1.1. Bedeutung von Cyber- und Online-Sicherheit

Cybersicherheit ist nicht nur ein Modewort

Es ist ein Schutzschild, das uns vor verschiedenen Online-Risiken schützt, darunter Identitätsdiebstahl, Finanzbetrug, Diebstahl persönlicher Daten, Cyberangriffe, die ein ganzes Unternehmen lahm legen, usw.

Cybersicherheit ist ein dreifacher Schutz

Im Pflegesektor hat die Cybersicherheit die Aufgabe, einzelne Pflegekräfte, ihre Organisationen und ihre Patient:innen zu schützen.

Cyberangriffe sind die neue Kriminalität

Wie die jüngste Welle von Ransomware-Angriffen auf Pflegeeinrichtungen (Krankenhäuser, Altenheime usw.) gezeigt hat, werden Cyberangriffe im Pflegesektor immer gefährlicher und bedrohlicher.

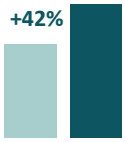
Schlussfolgerung: Die **Gefahr** der Cyberkriminalität war noch nie so existenziell wie heute. Unsere **Abhängigkeit** von digitalen Werkzeugen in allen Lebensbereichen macht uns zu **verwundbaren** Zielen, solange wir keine **Maßnahmen ergreifen**, um unsere digitale Sicherheit zu gewährleisten.

Co-funded by the European Union

1. Grundlagen Cyber- und Online-Sicherheit

1.1. Bedeutung von Cyber- und Online-Sicherheit

Ein paar Zahlen aus dem "Cyber Attack Trends: 2022 Mid-Year Report" zeigen, dass die Gefahr real ist. Allein im Jahr 2022:



Cyberangriffe auf Einrichtungen des Gesundheitswesens stiegen im Vergleich zum vorangegangenen Zeitraum um **42 %.**

Datenschutzverletzungen im Gesundheitswesen hatten durchschnittliche Gesamtkosten von **10,10 Millionen US-Dollar** pro Vorfall.

Gesundheitseinrichtungen erlebten weltweit **1.426** (dokumentierte) **Angriffe pro Woche**

1 von 42 Gesundheitseinrichtungen war im dritten Quartal 2022 Opfer eines Ransomware-Angriffs

Schlussfolgerung: Die **Gefahr** der Cyberkriminalität war noch nie so existenziell wie heute. Unsere **Abhängigkeit** von digitalen Werkzeugen in allen Lebensbereichen macht uns zu **verwundbaren** Zielen, solange wir keine **Maßnahmen ergreifen**, um unsere digitale Sicherheit zu gewährleisten.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s. · MPA · MedicalCare · åpenhet · Co-funded by the European Union

1. Grundlagen Cyber- und Online-Sicherheit

1.2. Verständnis von Pflegekräften für ihre Verantwortung in Bezug auf sensible Patient:innendaten

Vertrauen ist der Eckpfeiler und die Grundlage der Beziehung zwischen Pflegepersonal und Patient:in. Ein zentraler Bestandteil dieses Vertrauens ist die Fähigkeit, mit den sensiblen und persönlichen Daten der Patient:innen verantwortungsvoll umzugehen und sie zu schützen.

Patient:innendaten sind eine wahre Fundgrube an **persönlichen** und oft **sensiblen** Informationen.

- Anamnese
- Behandlungsplan
- Lebenshygiene
- Kontaktangaben
- Sozialversicherungs-nummer

Mitarbeiter:innen in Pflegeberufen sind mit großen Mengen **persönlicher** und **gesundheitlicher** Daten betraut, die für eine **Vielzahl von Interessengruppen von** Interesse sein können, von Unternehmen, die Produkte verkaufen, bis hin zu Betrüger:innen, die nach leichten Opfern suchen.

Noch wichtiger ist, dass diese Daten, unabhängig von ihrem Wert, **persönlich** und **privat** sind. Die Mitarbeiter:innen in Pflegeberufen tragen eine große Verantwortung dafür und sind es den Patient^:innen, die ihnen ihre Daten anvertrauen, schuldig, dies zu tun.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s. · MPA · MedicalCare · åpenhet · Co-funded by the European Union

1. Grundlagen Cyber- und Online-Sicherheit

1.2. Verständnis von Pflegekräften für ihre Verantwortung in Bezug auf sensible Patient:innendaten

Die digitale Verarbeitung von Patient:innendaten hat zwar das Leben der Pflegekräfte erleichtert und ihre Effizienz erhöht, stellt aber auch eine **Schwachstelle** und einen **neuen Bereich dar, der geschützt werden muss**.

Was ist mit GDPR? HIPAA?

Es gibt **gesetzliche Verpflichtungen**, um ein Mindestmaß an Schutz zu gewährleisten und eine Bewegung in Gang zu setzen. Das Pflegepersonal sollte jedoch nicht nur deshalb Datenschutzmaßnahmen ergreifen, um diesen Verpflichtungen nachzukommen: Es ist eine **ethische Pflicht**, die **Würde** und **Privatsphäre** der Patient:innen zu wahren.

Der Datenschutz geht über die Einhaltung der gesetzlichen Verpflichtungen hinaus.

Das Pflegepersonal muss sich der **Auswirkungen** bewusst sein, die **Datenschutzverletzungen** haben können, und das **Gewicht und die Bedeutung** seiner **Verantwortung** verstehen. Das Vertrauen der Patient:innen hängt von dieser Erkenntnis ab, ebenso wie die moralische Verpflichtung der Pflegekräfte, ihre Patient:innen zu schützen.

Co-funded by the European Union

1. Grundlagen Cyber- und Online-Sicherheit

1.3. Menschliche Fehler und Nachlässigkeit als Haupteinfallstor für Cyber-Kriminalität

Menschliche Fehler und Nachlässigkeit sind es, die Cyberkriminelle ausnutzen. Sie stellen das einfachste **Einfallstor** dar und sind so, als würde man nachts beim Verlassen einer Pflegeeinrichtung die Tür ohne Überwachung weit offen stehen lassen.

Das Hacken von Software und Datenbanken durch Ausnutzung **technischer Schwachstellen** gibt es zwar, aber es ist sehr selten und macht nur einen kleinen Teil der Cyberangriffe aus. In der überwiegenden Mehrheit der Fälle gehen Cyberkriminelle einfach durch die von Menschen - entweder durch Fehler oder Nachlässigkeit - **offen gelassenen Türen**, um **sich unbefugt Zugang zu** verschaffen und **sensible Informationen zu missbrauchen**.

"Ich bin Pflegekraft, kein Nerd. Warum sollte mich das interessieren?"

Bei fast allen Cyberangriffen, die in letzter Zeit im Gesundheitswesen aufgetreten sind (Phishing, Ransomware usw.), war die Ursache für den Einbruch nicht ein defektes Antivirusprogramm, eine schwache Software oder eine suboptimale technische Architektur: Diese Angriffe nutzen fast immer **menschliche Fehler** aus, die häufig vom medizinischen Personal selbst verursacht werden.

Co-funded by the European Union

1. Grundlagen Cyber- und Online-Sicherheit

1.4. Was können wir tun?
Schwachstellen beim Menschen erkennen und behandeln

Bei der Cybersicherheit im Pflegesektor geht es nicht nur um individuelle Bemühungen – die Fehler Einzelner haben Auswirkungen auf alle anderen. Es geht um **kollektive Verantwortung**, **Sensibilisierung**, Umsetzung **bewährter Verfahren** und **Schulungen**.

Cybersicherheit ist ein institutionell komplexes Thema, da sich die Fehler Einzelner auf alle auswirken (wie das Beispiel der Ransomware zeigt, der viele Krankenhäuser zum Opfer gefallen sind). Aufgrund dieses allumfassenden Charakters geht es bei der Cybersicherheit um die **Verbesserung der kollektiven Verteidigung** gegen Cyber-Bedrohungen und nicht nur um die Verbesserung individueller Verhaltensweisen.

Dies bedeutet, dass **gemeinsame Anstrengungen unternommen werden müssen**, um **das Bewusstsein zu schärfen, die Verantwortung und die Eigenverantwortung zu erhöhen, die Mitarbeiter:innen** über Cyber-Bedrohungen **aufzuklären**, gemeinsam Prozesse einzuführen und anzuwenden, die **bewährte Verfahren** integrieren, usw.

Auf **individueller Ebene** bedeutet Cybersicherheit nicht nur die **Einhaltung von Protokollen** und Prozessen, sondern auch das Verständnis der eigenen Position als **Akteur der Cybersicherheit der Institution**, was **kritisches Denken und Sensibilisierung** für Gefahren, Beiträge zu **Schulungen oder Mentoring** sowie **aktive Beteiligung** und Eigenverantwortung voraussetzt.

1. Grundlagen Cyber- und Online-Sicherheit

1.4. Was können wir tun?
Schwachstellen beim Menschen erkennen und behandeln

Cybersicherheit ist eine unsichere Wissenschaft: Auch in gut geschützten und gut ausgebildeten Strukturen kommt es zu Sicherheitsverletzungen. **Korrekturmaßnahmen und vorbereitet sein für den** Fall von Sicherheitsverletzungen sollten von Organisationen nicht vernachlässigt werden.

Selbst mit einem verbesserten Ansatz für Cybersicherheit, besseren Prozessen, besser ausgebildeten Mitarbeiter:innen usw. kann es immer noch zu Datenschutzverletzungen und Cyberangriffen kommen, wenn auch in deutlich geringerem Umfang. Einen 100-prozentigen Schutz gibt es nicht, und daher ist es für Pflegeeinrichtungen von entscheidender Bedeutung, über umfassende Strategien zu verfügen, die im Falle von Verstößen unverzüglich umgesetzt werden können, und auf Krisenmanagement, Gegenmaßnahmen, Wiederherstellung der Kontrolle und Verringerung der Auswirkungen vorbereitet zu sein.

Diese Strategien sind jedoch eher auf der Ebene der **technischen Teams zu** entwickeln und implizieren einen **spezifischeren, technischen Inhalt**. Korrekturmaßnahmen und Bereitschaft sind also nicht Teil dieses Lehrplans, obwohl sie für jede Pflegeorganisation absolut notwendig sind.

Co-funded by the European Union

2. Überblick über die häufigsten Bedrohungen

1. Schutz von Patient:innen
2. Phishing-Angriffe
3. Malware
4. Social Engineering

2. Überblick über die häufigsten Bedrohungen

2.1. Schutz von Patient:innen

Online-Bedrohungen können gezielt eingesetzt werden und schaden

Einzelne Mitarbeitende

Pflege-organisationen

Patient:innen

Dies gilt insbesondere für bestimmte Patient:innenkategorien, die einem höheren **Risiko ausgesetzt sind**, Opfer von Cyberangriffen zu werden, wie etwa **isolierte ältere Menschen**.

Pflegekräfte können ihre Patient:innen schützen, wenn sie ein Online-Risiko für deren Sicherheit erkennen, indem sie

Beobachtung ihres Online-Verhaltens

Mit ihnen diskutieren und sie über ihr Online-Leben befragen

Erkennen potenzieller Risiken in ihrem Online-Verhalten

Warnung vor erkannten Gefahren

Aufklärung über Online-Sicherheit

2. Überblick über die häufigsten Bedrohungen

2.2. Phishing-Angriffe

Phishing-Angriffe sind **betrügerische** Versuche, **an sensible Informationen zu gelangen**, indem sie sich als **vertrauenswürdige** Einrichtungen ausgeben. Im Pflegesektor können Phishing-Angriffe vor allem in folgender Form auftreten:

E-Mail-Betrügereien für Unternehmen ("Whaling")

Ausgeklügelte Angriffe, die darauf abzielen, Mitarbeiter:innen zur Überweisung von Geldern oder zur Preisgabe sensibler Informationen zu **verleiten**.

Diese Betrügereien werden oft per **E-Mail** an Finanz- oder Buchhaltungsabteilungen gestartet, indem sie **sich als** hochrangige Führungskräfte oder autorisierte Mitarbeiter:innen **ausgeben**.

From: CEO@acmecorp.com
To: Jane@acmecorp.com
Subject: Urgent

I need you to initiate a wire transfer in the sum of $45,250 to the account below. I am boarding a flight and this needs to be done right now. Can you please get this done? Send confirmation of the transfer immediately.

Thanks

Quelle: Proofpoint

2. Überblick über die häufigsten Bedrohungen

2.2. Phishing-Angriffe

Phishing-Angriffe sind **betrügerische** Versuche, **an sensible Informationen zu gelangen**, indem sie sich als **vertrauenswürdige** Einrichtungen ausgeben. Im Pflegesektor können Phishing-Angriffe vor allem in folgender Form auftreten:

Diese Phishing-E-Mails fordern in der Regel **dringende** Zahlungen, Änderungen von Lieferantendaten oder vertrauliche Mitarbeiter:inneninformationen an und nutzen dabei die **hierarchische Beziehung** zwischen Absender:in und Empfänger:in aus.

HINWEISE

- ✓ Absender:in verwendet höhere hierarchische Position
- ✓ Gefühl der Dringlichkeit - keine Zeit zum Prüfen / Protestieren
- ✓ Sender:in kann nicht telefonieren, nur schreiben
- ✓ Gefälschter Domänenname der Absender:in-E-Mail

2. Überblick über die häufigsten Bedrohungen

2.2. Phishing-Angriffe

Phishing-Angriffe sind **betrügerische** Versuche, **an sensible Informationen zu gelangen**, indem sie sich als **vertrauenswürdige** Einrichtungen ausgeben. Im Pflegesektor können Phishing-Angriffe vor allem in folgender Form auftreten:

Phishing-Angriffe zum Sammeln von Anmeldeinformationen

Phishing-Angriffe zum Sammeln von Anmeldedaten zielen darauf ab, Benutzernamen, Kennwörter und andere **Anmeldedaten zu stehlen**, um sich **unbefugten Zugang** zu Pflegesystemen zu verschaffen. Diese Betrügereien verwenden oft überzeugende **Nachbildungen** legitimer Anmeldeseiten, wie EMR-Portale oder Intranets.

Angreifer:innen versenden Phishing-E-Mails oder leiten die Opfer auf **gefälschte Websites**, wo sie ihre Anmeldedaten eingeben und so **unwissentlich den** Cyberkriminellen den Schlüssel zu den vertraulichen Daten ihres Unternehmens überlassen.

HINWEISE

- ✓ Gefälschter Domänenname der Absender:in-E-Mail (z. B. @msupdate.net)
- ✓ Abweichendes Design der E-Mail von den üblichen E-Mails des Unternehmens
- ✓ Aufforderung, auf etwas zu reagieren, was Sie nicht getan haben (z. B. ein Paket zu liefern, das Sie nicht bestellt haben).

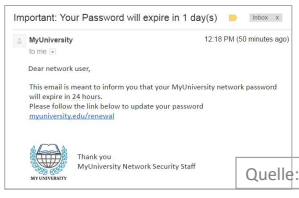
2. Überblick über die häufigsten Bedrohungen

2.2. Phishing-Angriffe

Phishing-Angriffe sind **betrügerische** Versuche, **an sensible Informationen zu gelangen**, indem sie sich als **vertrauenswürdige** Einrichtungen ausgeben. Im Pflegesektor können Phishing-Angriffe vor allem in folgender Form auftreten:

Malware-beladene Phishing-E-Mails

Mit Malware verseuchte Phishing-E-Mails sollen die Empfänger:innen zum Herunterladen und Ausführen von **Schadsoftware verleiten**. Diese E-Mails enthalten oft **infizierte Anhänge** oder **Links** zu gefährdeten Websites.
Organisationen des **Gesundheitswesens** sind **besonders anfällig** für Malware-Angriffe, da erfolgreiche Angriffe Patient:innendaten missbrauchen, den Betrieb stören oder sogar Menschenleben gefährden können.



Quelle: Imperva

HINWEISE

- ✓ Rechtschreib-, Grammatik- und Zeichensetzungsfehler
- ✓ Links im Text der E-Mail, die zu unerwarteten Websites weiterleiten (fahren Sie mit dem Mauszeiger über den Link, um die URL anzuzeigen)
- ✓ Bedrohung (z. B. gesperrtes Konto) oder Gefühl der Dringlichkeit
- ✓ Anhänge, die Sie nicht angefordert haben
- ✓ Ungewöhnliche Anfrage, ungewöhnlicher Ton oder ungewöhnliche Begrüßung

Co-funded by the European Union

2. Überblick über die häufigsten Bedrohungen

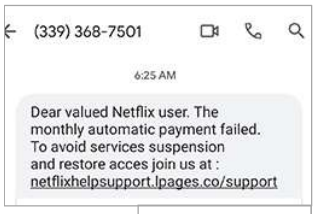
2.2. Phishing-Angriffe

Phishing-Angriffe sind **betrügerische** Versuche, **an sensible Informationen zu gelangen**, indem sie sich als **vertrauenswürdige** Einrichtungen ausgeben. Im Pflegesektor können Phishing-Angriffe vor allem in folgender Form auftreten:

Vishing- und Smishing-Angriffe

Vishing (durch Sprachnachrichten oder Telefonanrufe) und **Smishing** (durch SMS) können alle bisherigen Phishing-Angriffe sein. Sie ersetzen einfach die traditionelle E-Mail durch ein anderes Kommunikationsmittel (SMS, Anruf usw.).

Quelle: FR Sicher



Quelle: Devfuzion

2. Überblick über die häufigsten Bedrohungen

2.2. Phishing-Angriffe

Phishing-Angriffe sind **betrügerische** Versuche, **an sensible Informationen zu gelangen**, indem sie sich als **vertrauenswürdige** Einrichtungen ausgeben. Im Pflegesektor können Phishing-Angriffe vor allem in folgender Form auftreten:

HINWEISE

Vishing

- ✓ Fordernder Ton: Betrüger:innen nutzen Angst oder Panik aus
- ✓ Ersuchen um vertrauliche oder persönliche Informationen
- ✓ Anrufer:in: Die meisten Organisationen, die Betrüger:innen vorgeben zu vertreten, würden nicht bei Ihnen anrufen.

Smishing

- ✓ Unbekannte Nummer, nicht im Internet referenziert
- ✓ Besuchen Sie die Website des/der angeblichen Absenders/in - z. B. schreiben Banken auf ihren Websites, dass sie keine SMS verschicken.
- ✓ Wenden Sie sich direkt an den Kundendienst des Unternehmens

2. Überblick über die häufigsten Bedrohungen

2.2. Phishing-Angriffe

Phishing-Angriffe sind **betrügerische** Versuche, **an sensible Informationen zu gelangen**, indem sie sich als **vertrauenswürdige** Einrichtungen ausgeben. Im Pflegesektor können Phishing-Angriffe vor allem in folgender Form auftreten:

3.4 B

Phishing ist die am **weitesten verbreitete Form der Internetkriminalität**. Schätzungsweise **3,4 Milliarden E-Mails pro Tag** sind Phishing-Angriffe, die von Cyberkriminellen verschickt werden. Das sind über eine **Billion** Phishing-E-Mails pro **Jahr**.

36 %

36 % aller Datenschutzverletzungen gehen auf Phishing zurück.

E-Mail-Imitationen machen schätzungsweise **1,2 % des gesamten E-Mail-Verkehrs** weltweit aus.

1.2 %

84 %

84 % der Unternehmen waren im Jahr 2022 Ziel von mindestens **einem Phishing-Versuch**

Die durchschnittliche Klickrate für eine Phishing-Kampagne liegt bei **17,8 %.**

17.8%

3 %

Im Durchschnitt klicken 3 % der Mitarbeiter:innen auf einen bösartigen Link in einer Phishing-E-Mail.

2. Überblick über die häufigsten Bedrohungen

2.2. Phishing-Angriffe

Phishing-Angriffe sind **betrügerische** Versuche, **an sensible Informationen zu gelangen**, indem sie sich als **vertrauenswürdige** Einrichtungen ausgeben. Im Pflegesektor können Phishing-Angriffe vor allem in folgender Form auftreten:

91 %

aller Cyberangriffe beginnen mit einer **Phishing-E-Mail**

32.4 %

der **ungeschulten** Mitarbeiter:innen können auf Phishing-Betrug hereinfallen

95 %

der erfolgreichen Verstöße werden direkt durch **menschliches Versagen** verursacht

+ 350 %

Kleine Unternehmen sind zu **350 %** häufiger **Ziel** von **Phishing** als größere Unternehmen

0.1 %

0,1 % aller E-Mail-basierten Phishing-Angriffe sind für **66 %** aller Sicherheitsverletzungen verantwortlich (*in der Regel gezielte, personalisierte "Spear-Phishing"-Angriffe*)

66 %

Co-funded by the European Union

2. Überblick über die häufigsten Bedrohungen

2.3. Malware

Malware ist ein Überbegriff, der verschiedene Arten von Schadsoftware umfasst, die darauf abzielt, Computersysteme, Netzwerke oder Geräte zu stören, zu beschädigen oder sich Zugang zu ihnen zu verschaffen. Im Pflegebereich treten Malwares meist in Form von:

Viren

Viren sind bösartige Programme, die andere Dateien oder Software auf einem Computer **infizieren** und sich selbst replizieren, wenn die infizierten Dateien **ausgeführt werden**. Sie können Daten, Software und Hardwarekomponenten beschädigen.

So können beispielsweise mit Malware verseuchte Phishing-E-Mails oder SMS die Benutzer dazu verleiten, auf **Links zu** klicken oder infizierte **Dateien** herunterzuladen. Diese infizierten Dateien oder Links werden erst dann "aktiviert", wenn Benutzer:innen darauf klickt, daher ist beim Empfang unerbetener E-Mails Vorsicht geboten.

2. Überblick über die häufigsten Bedrohungen

2.3. Malware

Malware ist ein Überbegriff, der verschiedene Arten von Schadsoftware umfasst, die darauf abzielt, Computersysteme, Netzwerke oder Geräte zu stören, zu beschädigen oder sich Zugang zu ihnen zu verschaffen. Im Pflegebereich treten Malwares meist in Form von:

VORSICHT

Viele Betrüger:innen nutzen Ihre **Angst vor Viren** aus, um Sie zu infizieren: Wenn eine Popup-Meldung eines Antivirenprogramms, das Sie nicht besitzen, eine mögliche Infektion Ihres Geräts anzeigt und Ihnen anbietet, diese durch Klicken auf eine Schaltfläche oder durch Anrufen einer Nummer zu beheben, reagieren Sie nicht darauf, da dies sehr wohl dazu führen kann, dass Sie einen Virus ausführen.

Quelle: Microsoft-Gemeinschaft

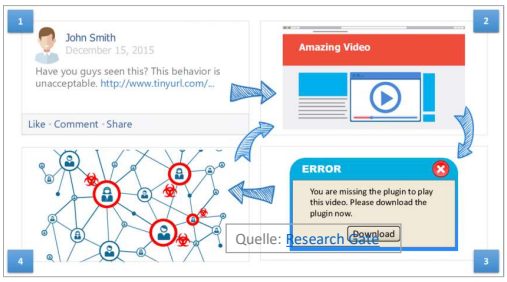
2. Überblick über die häufigsten Bedrohungen

2.3. Malware

Malware ist ein Überbegriff, der verschiedene Arten von Schadsoftware umfasst, die darauf abzielt, Computersysteme, Netzwerke oder Geräte zu stören, zu beschädigen oder sich Zugang zu ihnen zu verschaffen. Im Pflegebereich treten Malwares meist in Form von:

Trojaner

Trojaner oder trojanische Pferde sind **als legitime Software getarnte** Schadprogramme. Sie verleiten Benutzer:innen dazu, sie zu installieren, indem sie sich oft als harmlose Dateien oder Anwendungen tarnen. Sobald sie installiert sind, können Trojaner verschiedene bösartige Aktivitäten ausführen, z. B. sensible Daten stehlen, Informationen verändern oder Angreifern unbefugten Zugang verschaffen. Trojaner werden oft durch Phishing-E-Mails oder -Nachrichten ausgelöst.



2. Überblick über die häufigsten Bedrohungen

2.3. Malware

Malware ist ein Überbegriff, der verschiedene Arten von Schadsoftware umfasst, die darauf abzielt, Computersysteme, Netzwerke oder Geräte zu stören, zu beschädigen oder sich Zugang zu ihnen zu verschaffen. Im Pflegebereich treten Malwares meist in Form von:

HINWEISE

- ✓ Der Computer läuft langsamer als sonst.
- ✓ Nicht autorisierte Anwendungen werden auf dem Gerät angezeigt.
- ✓ Häufige Abstürze und Einfrieren des Geräts.
- ✓ Häufige Pop-ups.
- ✓ Einige Anwendungen lassen sich nicht starten.
- ✓ Häufige Unterbrechungen der Internetverbindung.

Co-funded by the European Union

2. Überblick über die häufigsten Bedrohungen

2.3. Malware

Malware ist ein Überbegriff, der verschiedene Arten von Schadsoftware umfasst, die darauf abzielt, Computersysteme, Netzwerke oder Geräte zu stören, zu beschädigen oder sich Zugang zu ihnen zu verschaffen. Im Pflegebereich treten Malwares meist in Form von:

Ransomware

Ransomware ist eine Art von Malware, die Dateien auf dem Computer oder Gerät eines Opfers verschlüsselt und sie **unzugänglich** macht, **bis ein Lösegeld gezahlt wird**. Ransomware-Angriffe verlangen in der Regel eine Zahlung in Kryptowährung und können erhebliche finanzielle und Datenverluste verursachen.

Krankenhäuser und Einrichtungen des Gesundheitswesens, deren Systeme für ihren Betrieb unerlässlich sind, sind besonders betroffen. Im Jahr 2022 waren **66 %** der Krankenhäuser in den USA das **Ziel** (nicht immer das Opfer) eines Ransomware-Angriffs. In etwa **61 %** der Ransomware-Vorfälle im Jahr 2022 **zahlten** Organisationen des Gesundheitswesens das Lösegeld.

Quelle: Healthcare IT News

2. Überblick über die häufigsten Bedrohungen

2.3. Malware

Malware ist ein Überbegriff, der verschiedene Arten von Schadsoftware umfasst, die darauf abzielt, Computersysteme, Netzwerke oder Geräte zu stören, zu beschädigen oder sich Zugang zu ihnen zu verschaffen. Im Pflegebereich treten Malwares meist in Form von:

Würmer

Würmer sind eigenständige Malware-Programme, die sich in Netzwerken **replizieren** und in der Regel Schwachstellen in Betriebssystemen oder Netzwerkprotokollen ausnutzen.

Sie können sich schnell verbreiten und eine **Überlastung des Netzes** verursachen oder andere bösartige Aktivitäten durchführen.

Spionageprogramme

Spionageprogramme dienen der **heimlichen Überwachung** und Sammlung von Informationen über die Aktivitäten von Benutzer:innen auf deren Computer oder Gerät.

Sie können **Tastatureingaben verfolgen, Screenshots aufnehmen, Surfgewohnheiten aufzeichnen** und **vertrauliche Informationen** wie Passwörter und Finanzdaten stehlen.

Addwares

Bei Addwares handelt es sich um unerwünschte Software, die **Werbung** anzeigt, oft in Form von Popup-Werbung oder Browser-Weiterleitungen.

Adware ist zwar nicht per se bösartig, kann aber **die Systemleistung beeinträchtigen**, die **Privatsphäre von** Benutzer:innen gefährden und zu **weiteren Infektionen** führen, wenn sie nicht entfernt wird.

2. Überblick über die häufigsten Bedrohungen

2.3. Malware

Malware ist ein Überbegriff, der verschiedene Arten von Schadsoftware umfasst, die darauf abzielt, Computersysteme, Netzwerke oder Geräte zu stören, zu beschädigen oder sich Zugang zu ihnen zu verschaffen. Im Pflegebereich treten Malwares meist in Form von:

Keylogger

Keylogger sind eine Art von Spyware, die von Benutzer:innen getippte **Tastenanschläge** aufzeichnen und so vertrauliche Informationen wie **Kennwörter**, **Benutzernamen** und Kreditkartendaten erfassen.

Angreifer:innen können Keylogger verwenden, um persönliche Daten zu stehlen und Identitätsdiebstahl zu begehen.

Botnetze

Botnets sind **Netzwerke aus kompromittierten Computern** oder Geräten, die von Angreifer:innen kontrolliert werden.

Botnets können dazu verwendet werden, verteilte Denial-of-Service-Angriffe **(DDoS) durchzuführen, Spam-E-Mails** zu versenden oder andere bösartige Aktivitäten **ohne das Wissen der Besitzer:innen** durchzuführen.

Hintertüren

Hintertüren sind **versteckte Einstiegspunkte** oder Schwachstellen, die von Angreifer:innen absichtlich in Software oder Systemen geschaffen werden, um **unbefugten Zugriff für eine spätere Zugriffe oder Kontrolle zu** ermöglichen. Diese Hintertüren ermöglichen es Angreifern, **heimlich und aus der Ferne** die Kontrolle über das Gerät zu übernehmen, andere Schadprogramme zu installieren, Tastenanschläge aufzuzeichnen usw.

Co-funded by the European Union

2. Überblick über die häufigsten Bedrohungen

2.3. Malware

Diese verschiedenen Arten von Malware sind oft in einem Programm oder einer Datei kombiniert. Ein paar Zahlen aus dem Jahr **2022** zeigen, wie verbreitet, ausgefeilt und gefährlich Malware ist (Quelle: Getastra.com)

1 Milliarde

Täglich werden 560 000 neue Malware-Programme entdeckt. Derzeit gibt es über **1 Milliarde** Malware-Programme.

$4.5 M

Jede Minute werden **4 Unternehmen** Opfer von Ransomware-Angriffen. Der **Pflegesektor** ist am stärksten betroffen und zahlt das meiste Lösegeld. Die durchschnittlichen Kosten eines Ransomware-Angriffs liegen bei **4,54 Millionen Dollar.**

50%

Bei Ransomware-Vorfällen konnten nur **50 %** der Unternehmen, die **Lösegeld** gezahlt hatten, **ihre Daten wiederherstellen**. **64 %** der Unternehmen, die Ziel von Ransomware-Angriffen waren, wurden tatsächlich **infiziert**.

+87%

In den letzten zehn Jahren ist die Zahl der Malware-Infektionen **um 87 % gestiegen**. **Trojaner machen 58 %** der gesamten Computerschädlinge aus. Die Kosten der Cyberkriminalität werden für **das Jahr 2023 auf 8 Billionen Dollar** geschätzt.

Co-funded by the European Union

2. Überblick über die häufigsten Bedrohungen

2.4. Social Engineering

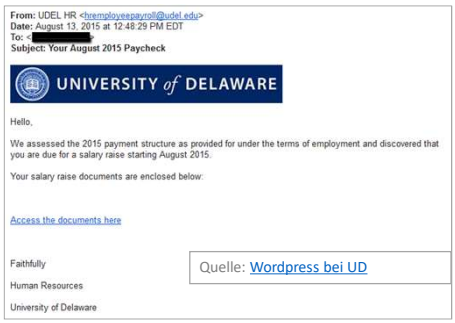
Social Engineering bezieht sich auf den Einsatz sozialer Taktiken, um das Vertrauen, die Nachlässigkeit oder die Unwissenheit von Mitarbeiter:innen auszunutzen, um an vertrauliche Informationen zu gelangen. Während Phishing- und Malware-Angriffe diese Schwachstellen häufig ausnutzen und **sich** mit Social Engineering **überschneiden**, werden bei reinem Social Engineering eher **soziale Taktiken** eingesetzt, die Folgendes beinhalten können:

Spear-Phishing

Spear-Phishing ist eine **gezielte Form des Phishings**, bei der **der Angriff** auf bestimmte Personen oder Organisationen **zugeschnitten ist**.

Die Angreifer:innen sammeln Informationen über ihre Ziele aus sozialen Medien, öffentlichen Datenbanken oder früheren Interaktionen, um die Phishing-E-Mails zu personalisieren und die Erfolgswahrscheinlichkeit zu erhöhen.

Spear-Phishing-Nachrichten können verschiedene Arten von Malware enthalten, direkt persönliche Daten abfragen (z. B. die Telefonnummer, um eine "dringende Angelegenheit" zu klären), zur Zahlung einer Rechnung auffordern usw.


From: UDEL HR <hremployeepayroll@udel.edu>
Date: August 13, 2015 at 12:48:29 PM EDT
To: [redacted]
Subject: Your August 2015 Paycheck

UNIVERSITY of DELAWARE

Hello,

We assessed the 2015 payment structure as provided for under the terms of employment and discovered that you are due for a salary raise starting August 2015.

Your salary raise documents are enclosed below:

Access the documents here

Faithfully

Human Resources

University of Delaware

Quelle: Wordpress bei UD

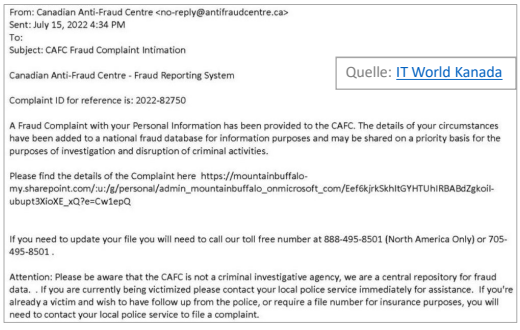
2. Überblick über die häufigsten Bedrohungen

2.4. Social Engineering

Social Engineering bezieht sich auf den Einsatz sozialer Taktiken, um das Vertrauen, die Nachlässigkeit oder die Unwissenheit von Mitarbeiter:innen auszunutzen, um an vertrauliche Informationen zu gelangen. Während Phishing- und Malware-Angriffe diese Schwachstellen häufig ausnutzen und **sich** mit Social Engineering **überschneiden**, werden bei reinem Social Engineering eher **soziale Taktiken** eingesetzt, die Folgendes beinhalten können:

Pretexting

Beim Pretexting wird ein **erfundenes Szenario oder ein Vorwand** geschaffen, um Personen dazu zu bringen, vertrauliche Informationen preiszugeben oder bestimmte Handlungen auszuführen.
Angreifer:innen geben sich oft als **vertrauenswürdige Personen aus**, z. B. als IT-Support-Mitarbeiter:innen, Strafverfolgungsbeamt:innen oder Führungskräfte eines Unternehmens, um das Vertrauen der Zielperson zu gewinnen und an vertrauliche Informationen zu gelangen. Vorgetäuschte Betrügereien können zu sehr ähnlichen Ergebnissen führen wie jede Art von Phishing-Betrug: Zahlungsaufforderung, Diebstahl von Anmeldeinformationen oder persönlichen Daten usw.


From: Canadian Anti-Fraud Centre <no-reply@antifraudcentre.ca>
Sent: July 15, 2022 4:34 PM
To:
Subject: CAFC Fraud Complaint Intimation

Canadian Anti-Fraud Centre - Fraud Reporting System

Quelle: IT World Kanada

Complaint ID for reference is: 2022-82750

A Fraud Complaint with your Personal Information has been provided to the CAFC. The details of your circumstances have been added to a national fraud database for information purposes and may be shared on a priority basis for the purposes of investigation and disruption of criminal activities.

Please find the details of the Complaint here https://mountainbuffalo-my.sharepoint.com/:u:/g/personal/admin_mountainbuffalo_onmicrosoft_com/Eef6kjrkSkhltGYHTUhIRBABdZgkoil-ubupt3XioXE_xQ?e=Cw1epQ

If you need to update your file you will need to call our toll free number at 888-495-8501 (North America Only) or 705-495-8501 .

Attention: Please be aware that the CAFC is not a criminal investigative agency, we are a central repository for fraud data. . If you are currently being victimized please contact your local police service immediately for assistance. If you're already a victim and wish to have follow up from the police, or require a file number for insurance purposes, you will need to contact your local police service to file a complaint.

2. Überblick über die häufigsten Bedrohungen

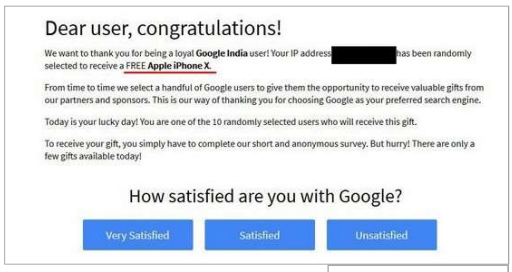
2.4. Social Engineering

Social Engineering bezieht sich auf den Einsatz sozialer Taktiken, um das Vertrauen, die Nachlässigkeit oder die Unwissenheit von Mitarbeiter:innen auszunutzen, um an vertrauliche Informationen zu gelangen. Während Phishing- und Malware-Angriffe diese Schwachstellen häufig ausnutzen und **sich** mit Social Engineering **überschneiden**, werden bei reinem Social Engineering eher **soziale Taktiken** eingesetzt, die Folgendes beinhalten können:

Köder

Köder nutzen die **Neugier oder Gier** von Personen aus, um sie zum Herunterladen bösartiger Dateien oder zum Besuch kompromittierter Websites zu verleiten. Angreifer:innen bieten **verlockende Köder** an, wie z. B. kostenlose Software-Downloads, Film-Downloads oder Geschenkkarten, die Malware enthalten oder zu Phishing-Seiten führen, wenn sie aufgerufen werden.

Köder sind oft mit einer Art von Vorwand, Spear-Phishing, Impersonation usw. verbunden, um die **Schwachstellen** der Benutzer:innen auszunutzen und die **Glaubwürdigkeit** der Absender:innen zu erhöhen.



Quelle: Dummies.de

2. Überblick über die häufigsten Bedrohungen

2.4. Social Engineering

Social Engineering bezieht sich auf den Einsatz sozialer Taktiken, um das Vertrauen, die Nachlässigkeit oder die Unwissenheit von Mitarbeiter:innen auszunutzen, um an vertrauliche Informationen zu gelangen. Während Phishing- und Malware-Angriffe diese Schwachstellen häufig ausnutzen und **sich** mit Social Engineering **überschneiden**, werden bei reinem Social Engineering eher **soziale Taktiken** eingesetzt, die Folgendes beinhalten können:

Tailgating (Huckepackfahren):

Tailgating oder Huckepack bedeutet, dass man **sich physisch unbefugten Zugang** zu gesperrten Bereichen oder Systemen **verschafft**, indem man einer autorisierten Person folgt.

Angreifer:innen nutzen die **menschliche Höflichkeit oder mangelndes Bewusstsein** aus, um unbefugt in gesicherte Räumlichkeiten einzudringen.

Angriffe auf Wasserlöcher

Watering-Hole-Angriffe zielen auf bestimmte Gruppen oder Organisationen ab, indem sie **Websites, die von deren Mitgliedern besucht werden**, mit Malware **infizieren**.

Angreifer:innen kompromittieren legitime Websites, um **Malware** an ahnungslose Besucher:innen zu **verteilen** und deren Vertrauen in die kompromittierte Website auszunutzen.

Impersonation (Identitätsdiebstahl):

Die meisten Phishing-Taktiken beinhalten eine Form der Identitätsverschleierung. Einige enthalten jedoch zusätzliche Elemente zur Erhöhung der Glaubwürdigkeit, die einen **Identitätsdiebstahl** darstellen.

Dazu können gestohlene oder gefälschte Ausweise und Dokumente, von der IA erstellte Elemente usw. gehören, um über ihre Authentizität **zu täuschen**.

Co-funded by the European Union

2. Überblick über die häufigsten Bedrohungen

2.4. Social Engineering

Social Engineering bezieht sich auf den Einsatz sozialer Taktiken, um das Vertrauen, die Nachlässigkeit oder die Unwissenheit von Mitarbeiter:innen auszunutzen, um an vertrauliche Informationen zu gelangen. Während Phishing- und Malware-Angriffe diese Schwachstellen häufig ausnutzen und **sich** mit Social Engineering **überschneiden**, werden bei reinem Social Engineering eher **soziale Taktiken** eingesetzt, die Folgendes beinhalten können:

90 %

90 % der Datenschutzverletzungen und **98 %** der Cyberangriffe (erfolgreich oder nicht) hatten Social-Engineering-Elemente.

$4.5 M

Durch Social-Engineering-Techniken initiierte Datenschutzverletzungen verursachten im Durchschnitt **Kosten von über 4,5 Millionen Dollar**.

700

Ein typisches Unternehmen (in den USA) wurde **jedes Jahr** Ziel von über **700 Social-Engineering-Angriffen.**

+ 354 %

Die **Angriffe zur Übernahme von Konten** stiegen im Jahr 2023 um 354 % gegenüber dem Vorjahr.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s. · MPA · MedicalCare · åpenhet · Co-funded by the European Union

3. Vorbeugende Maßnahmen

1. Passwortsicherheit
2. Zwei-Faktor-Authentifizierung (2FA)
3. Antivirus
4. Software-Aktualisierungen
5. Sicherheit im Netz
6. Datensicherung

JIHOMĚSTSKÁ SOCIÁLNÍ a.s. · MPA · MedicalCare · åpenhet · Co-funded by the European Union

3. Vorbeugende Maßnahmen

3.1. Passwortsicherheit

Warum ist das wichtig?

Die Passwortsicherheit ist die **erste Schwachstelle**, die von Cyberkriminellen ausgenutzt wird. **Stärkere** Passwörter (d. h. kompliziertere und vielfältigere) sind schwerer zu erraten oder durch Brute-Force-Angriffe aufzudecken und können daher eine nützliche **erste Verteidigungslinie** gegen Cyberangriffe sein.

Was kann ich tun?

- Legen Sie **sichere** Passwörter fest: mindestens **16** Zeichen, mit Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.
- **Verwandeln Sie Sätze** in Passwörter statt in Wörter, indem Sie einen Code verwenden, um verschiedene Arten von Buchstaben umzuwandeln. Beispiel: "Ic**à**re@b0utSecur1ty!"
- Verwenden Sie **Passwort-Manager**, die sich Ihre Passwörter für Sie merken und Passwörter generieren.

Was kann meine Organisation tun?

- Konfigurieren Sie Ihre Systeme (E-Mail, Online-Messaging-Tools, ERP, CRM usw.) so, dass die Benutzer:innen gezwungen sind, **ihr Passwort regelmäßig zu erneuern.** Dies verkürzt die Zeit, in der ein bestimmtes Passwort gültig bleibt.
- Konfigurieren Sie **Kennwortregeln**, um sicherzustellen, dass Benutzer:innen **dasselbe Kennwort** nicht **zweimal** verwenden und dass das Kennwort **sicher genug ist**.
- Erzwingen Sie eine allgemeine **Kennworterneuerung** nach einer Sicherheitsverletzung.

3. Vorbeugende Maßnahmen

3.1. Passwortsicherheit

Warum ist das wichtig?

Die Passwortsicherheit ist die **erste Schwachstelle**, die von Cyberkriminellen ausgenutzt wird. **Stärkere** Passwörter (d. h. kompliziertere und vielfältigere) sind schwerer zu erraten oder durch Brute-Force-Angriffe aufzudecken und können daher eine nützliche **erste Verteidigungslinie** gegen Cyberangriffe sein.

ZOOM über Passwort-Manager

- Passwortmanager **speichern Ihre Passwörter** und entlasten Sie von der Pflicht, sich diese zu merken. Als Cloud-Lösungen bleiben sie **von anderen Geräten aus zugänglich**.
- Die Passwortregistrierung kann **manuell** oder **automatisch erfolgen.** Sie können den Passwortmanager auch so einstellen, dass er das Passwortfeld automatisch ausfüllt, wenn Sie sich mit Ihren Konten verbinden.
- Besser noch: Passwort-Manager können für jedes Ihrer Konten **eindeutige, sehr sichere Passwörter erstellen** und sie für Sie speichern. Sie brauchen sie nicht einmal zu kennen.
- Sie müssen sich nur **ein einziges, sehr sicheres Passwort** merken - dasjenige, mit dem Sie Zugang zum Passwort-Manager erhalten.

Nützliche Tools

- Dashlane
- 1Password
- LastPass
- Bitwarden

Co-funded by the European Union

3. Vorbeugende Maßnahmen

3.2. Zwei-Faktor-Authentifizierung (2FA)

Warum ist das wichtig?

2FA verbessert die Sicherheit drastisch: Diese Authentifizierungsmethode erfordert die Verwendung von mindestens **zwei Geräten**, um sich bei einem Konto anzumelden, wobei beide zuvor **registriert** und **vertrauenswürdig sein müssen**. Diese Methode gibt den Nutzer:innen nicht nur die **Kontrolle** über ein Konto, das möglicherweise kompromittiert wurde, sondern kann auch **anzeigen**, dass es kompromittiert wurde.

Was kann ich tun?

- **Aktivieren Sie 2FA** so früh wie möglich - wenn ein Passwort oder ein Konto kompromittiert wurde, ist es zu spät.
- In den meisten Softwareprogrammen und Websites finden Sie die Möglichkeit, diese Funktion unter **Einstellungen > Sicherheit** zu aktivieren (IOS und Microsoft, Google-Dienste, soziale Medien usw.).
- Die am häufigsten verwendete und zuverlässigste Methode ist die Verwendung von **zwei Geräten** des Nutzers (z. B. Telefon und Computer), die auf einem Konto registriert sind.

3. Vorbeugende Maßnahmen

3.2. Zwei-Faktor-Authentifizierung (2FA)

Warum ist das wichtig?

2FA verbessert die Sicherheit drastisch: Diese Authentifizierungsmethode erfordert die Verwendung von mindestens **zwei Geräten**, um sich bei einem Konto anzumelden, wobei beide zuvor **registriert** und **vertrauenswürdig sein müssen**. Diese Methode gibt dem Nutzer nicht nur die **Kontrolle** über ein Konto, das möglicherweise kompromittiert wurde, sondern kann auch **anzeigen**, dass es kompromittiert wurde.

Was kann meine Organisation tun?

- Bei den meisten Systemen kann Ihre IT-Abteilung die **2FA systemweit** für alle Benutzer:innen durchsetzen. 2FA kann auch als "zweistufige Verifizierung" oder "Multi-Faktor-Authentifizierung" bezeichnet werden.
- Dies setzt jedoch voraus, dass alle **Mitarbeiter:innen Zugang zu 2 Geräten haben**, die idealerweise nur für die berufliche Nutzung bestimmt sind, was möglicherweise nicht der Fall ist. Alternativ können die Mitarbeiter:innen **dazu angehalten werden**, 2FA zu aktivieren.

3. Vorbeugende Maßnahmen

3.2. Zwei-Faktor-Authentifizierung (2FA)

Warum ist das wichtig?

2FA verbessert die Sicherheit drastisch: Diese Authentifizierungsmethode erfordert die Verwendung von mindestens **zwei Geräten**, um sich bei einem Konto anzumelden, wobei beide zuvor **registriert** und **vertrauenswürdig sein müssen**. Diese Methode gibt dem Nutzer nicht nur die **Kontrolle** über ein Konto, das möglicherweise kompromittiert wurde, sondern kann auch **anzeigen**, dass es kompromittiert wurde.

Wie kann ich das tun?

- Google Workspace (Gmail, Gdrive, Kalender, etc.)
- Microsoft 365 (Outlook, OneDrive, Teams, usw.)
- Slack
- Zoom

Und andere - allgemein verfügbar im Bereich **Sicherheit der Einstellungen** für die meisten digitalen Tools - auch für den persönlichen Gebrauch (soziale Medien, Bankgeschäfte, elektronischer Handel, Anwendungen und Websites von Behörden usw.).

Co-funded by the European Union

3. Vorbeugende Maßnahmen

3.3. Antivirus

Warum ist das wichtig?

Antivirenprogramme schützen ihren Besitzer:innen, indem sie **potenzielle Bedrohungen scannen und Risiken erkennen**, von E-Mail-Phishing oder Malware-Versuchen bis hin zu betrügerischen Websites und Programmen. Dieser Schutz erstreckt sich nicht nur auf den Computer, sondern auch auf alle **externen Geräte,** die mit ihm interagieren, wie z. B. USB-Sticks, die ebenfalls mit Malware infiziert sein könnten.

Was kann ich tun?

- **Installieren Sie selbstständig** eine Antiviren-Software, wenn diese nicht von Ihrem Unternehmen bereitgestellt wird (oder **setzen Sie sich dafür ein**, dass dies unternehmensweit geschieht). Ungeschützte Computer sind ein **leichtes Ziel** für Cyberkriminelle.
- Denken Sie daran, dass Antivirenprogramme zusätzliche **Sicherheitsschichten** sind**, die immer noch vom menschlichen Faktor abhängen**: Seien Sie online **genauso wachsam**, ob Sie nun "geschützt" sind oder nicht.

Was kann meine Organisation tun?

Ihre IT-Abteilung kann und **sollte** Aktualisierungen einer **systemweiten Antiviren-Software** installieren, konfigurieren und verwalten, damit die digitale Sicherheit des Unternehmens besser geschützt ist.

Nützliche Tools

ESET
Kaspersky
Bitdefender
AVG

Co-funded by the European Union

3. Vorbeugende Maßnahmen

3.4. Software-Updates

Warum ist das wichtig?

Software und Betriebssysteme auf dem **neuesten Stand** zu halten, hindert Cyberkriminelle daran, bekannte **Sicherheitslücken** auszunutzen: Softwareanbieter führen regelmäßig Stresstests ihrer eigenen Sicherheit durch. Wenn sie potenzielle Sicherheitslücken entdecken, **bringen sie Updates heraus, die** diese Schwachstellen beseitigen oder nicht ausnutzbar machen.

Was kann ich tun?

Zögern Sie die Aktualisierung aller Software und Anwendungen, die Sie (privat und beruflich) nutzen, nicht hinaus, wenn Sie eine Update-Benachrichtigung erhalten. Vergewissern Sie sich regelmäßig, dass in Ihrem Anwendungszentrum alles auf dem neuesten Stand ist.

Was kann meine Organisation tun?

Ihre IT-Abteilung kann automatische Updates für Betriebssysteme und Anwendungen, die im gesamten Unternehmen verwendet werden, konfigurieren und auswählen, wann und wie oft sie installiert werden sollen, ohne den Betrieb zu unterbrechen.

3. Vorbeugende Maßnahmen

3.4. Software-Updates

Warum ist das wichtig?

Software und Betriebssysteme auf dem **neuesten Stand** zu halten, hindert Cyberkriminelle daran, bekannte **Sicherheitslücken** auszunutzen: Softwareanbieter führen regelmäßig Stresstests ihrer eigenen Sicherheit durch. Wenn sie potenzielle Sicherheitslücken entdecken, **bringen sie Updates heraus, die** diese Schwachstellen beseitigen oder nicht ausnutzbar machen.

Wie kann ich das tun?

Auf Windows

Auf Android

Auf dem Mac

Auf IOS

Nützliche Tools

Verwalten von Updates auf Windows

Automatische App-Updates einschalten

MacOS auf dem Mac aktualisieren

3. Vorbeugende Maßnahmen

3.5. Netzwerksicherheit - VPN

Warum ist das wichtig?

Wenn Mitarbeiter:innen von **außerhalb des Unternehmens** auf Informationen zugreifen müssen, wird es für das IT-Personal schwieriger, die **Kontrolle über alle Sicherheitsaspekte zu behalten**. **Virtuelle private Netze (VPN)** ermöglichen die Schaffung eines **direkten, sicheren und isolierten Netzes** zwischen zwei Rechnern, über das diese miteinander kommunizieren und Daten austauschen können.

Wie funktioniert das?

Ein VPN ist eine Technologie, die eine **sichere und verschlüsselte** Verbindung über das Internet herstellt. VPNs verschlüsseln Daten, die zwischen den Geräten von Nutzer:innen und dem VPN-Server übertragen werden, und verhindern so, dass Dritte die Daten abfangen und darauf zugreifen können. Diese Verschlüsselung ist eine **zusätzliche Sicherheitsebene**, die gewährleistet, dass sensible Informationen wie Passwörter, Kreditkartendaten und persönliche Mitteilungen sicher bleiben.

Im Zusammenhang mit Pflegepersonal werden VPNs vor allem **den Fernzugriff** auf private Netze und Ressourcen wie Firmenintranets, Server oder Datenbanken **sichern**, insbesondere für diejenigen, die im Außendienst arbeiten. Sie bieten auch **erhöhte Sicherheit** für diejenigen, die sich über **öffentliche** und im Allgemeinen ungesicherte **Wifi-Netzwerke** mit dem Internet verbinden.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s. · MEDICALCAR · åpenhet · Co-funded by the European Union

3. Vorbeugende Maßnahmen

3.5. Netzwerksicherheit - VPN

Warum ist das wichtig?

Wenn Mitarbeiter:innen von **außerhalb des Unternehmens** auf Informationen zugreifen müssen, wird es für das IT-Personal schwieriger, die **Kontrolle über alle Sicherheitsaspekte zu behalten**. **Virtuelle private Netze (VPN)** ermöglichen die Schaffung eines **direkten, sicheren und isolierten Netzes** zwischen zwei Rechnern, über das diese miteinander kommunizieren und Daten austauschen können.

Was kann meine Organisation tun?

VPNs sollten bei Bedarf von der **technischen Abteilung des Unternehmens** installiert werden, da sie meist als **systemweite geografische Erweiterung des bestehenden Netzes** genutzt werden und einzelne Benutzer:innen sie nicht eigenständig installieren können. Einzelpersonen können **sich** jedoch bei ihrer IT-Abteilung oder der Geschäftsleitung für ein VPN einsetzen.

VPNs können die **Installation einer Software** auf den zu verbindenden Rechnern sowie eine **Authentifizierungsmethode** vor dem Zugriff auf das Netz erfordern. Sie können so konfiguriert werden, dass sie nur auf bestimmten Geräten, an bestimmten Orten und zu bestimmten Zeiten funktionieren, um den Zugriff von außen einzuschränken, während sie den Mitarbeiter:innen, die sie benötigen, dennoch Zugang zu den erforderlichen Daten gewähren.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s. · MEDICALCAR · åpenhet · Co-funded by the European Union

3. Vorbeugende Maßnahmen

3.6. Datensicherung

Warum ist das wichtig?

Eine der größten Bedrohungen durch Cyberangriffe ist **die Veränderung sensibler Daten**, insbesondere von Patient:innendaten. Die Gewährleistung der Sicherheit und Integrität dieser Daten ist von absoluter Wichtigkeit, auch angesichts einer Cyberbedrohung. Eine solide **institutionelle Datensicherungsstrategie** mit regelmäßigen **Sicherungsverfahren** und einer **hohen Compliance der Mitarbeiter:innen** ist der Schlüssel zur Sicherung der Datenintegrität.

Was kann ich tun?

Für einzelne Arbeitnehmer:innen besteht die erste Maßnahme zur Gewährleistung der Datenintegrität und -sicherheit darin, die **verschiedenen** von der technischen Abteilung festgelegten **Protokolle einzuhalten**, **sich regelmäßig zu schulen** und **die Angelegenheit ernsthaft** und konsequent **anzugehen**.

- Als Akteur:innen der Sicherheit Ihres eigenen Unternehmens können Sie auch Ihre Datensicherungsstrategie **hinterfragen**, Änderungen **vorschlagen** und **befürworten**.

Was kann meine Organisation tun?

Die Ausarbeitung und Umsetzung einer **institutionellen Datensicherungsstrategie liegt in der** Verantwortung der technischen Abteilung. Eine solche Strategie sollte **Maßnahmen** umfassen, **die die Einhaltung der Vorschriften durch das Personal sicherstellen**, sowie Verfahren für die **regelmäßige Datensicherung** auf einer **Cloud-Speicherlösung** (Gdrive, Onedrive usw.) oder einem netzgebundenen Speicher, die ein Sicherheitsnetz für die **schnelle Wiederherstellung von Daten** im Falle einer Verletzung der Datenintegrität bieten.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s. · MedicalCare · åpenhet · Co-funded by the European Union

4. Best Practices - Empfehlungen

1. Sicheres Umfeld
2. Sicheres Surfen
3. Sicherer E-Mail-Versand
4. Sichere Nutzung sozialer Medien
5. Sicherheit mobiler Geräte
6. Passwortsicherheit

JIHOMĚSTSKÁ SOCIÁLNÍ a.s. · MedicalCare · åpenhet · Co-funded by the European Union

4. Best Practices - Empfehlungen

4.1. Sicheres Umfeld

Cybersicherheit beginnt offline: Bevor Sie technische Schutzmaßnahmen ergreifen, sollten Sie Ihren physischen Raum so organisieren, dass Gefahren und Schwachstellen reduziert werden.

1. Sperren Sie Ihre Geräte, wenn sie nicht benutzt werden
2. Sichern Sie Ihren Arbeitsbereich vor unbefugtem Zugriff
3. Führen Sie eine „Clean-Desk-Regel“ ein
4. Verwenden Sie Sichtschutzwänden
5. Vernichten Sie sensible Dokumente
6. Schreiben Sie keine Passwörter auf
7. Achten Sie auf “Schulter-Surfen”
8. Aktivieren Sie die Festplattenverschlüsselung

4. Best Practices - Empfehlungen

4.1. Sicheres Umfeld

Cybersicherheit beginnt offline: Bevor Sie technische Schutzmaßnahmen ergreifen, sollten Sie Ihren physischen Raum so organisieren, dass Gefahren und Schwachstellen reduziert werden.

1. Sperren Sie Ihre Geräte, wenn sie nicht benutzt werden

Schließen Sie Ihren Computer, Laptop, Ihr Tablet oder Telefon immer **ab**, wenn Sie es nicht benutzen, insbesondere in öffentlichen oder gemeinsam genutzten Räumen. Verwenden Sie starke Passwörter, PINs oder biometrische Authentifizierung (z. B. Fingerabdruck oder Gesichtserkennung), um Ihre Geräte zu sichern und unbefugten Zugriff zu verhindern.

Tipps

- Verwenden Sie unter Windows die Tastenkombination Windows + L, um Ihren Bildschirm zu sperren.
- Auf dem Mac verwenden Sie die Tastenkombination Strg-Befehl-Q, um Ihren Bildschirm zu sperren.

2. Sichern Sie Ihren Arbeitsbereich vor unbefugtem Zugriff

- Halten Sie Ihren Arbeitsbereich **frei von unbefugten Personen**. Stellen Sie sicher, dass Zugänge wie Türen, Fenster oder Eingänge gesichert und überwacht werden, um unbefugten Zutritt zu Ihrem Arbeitsbereich oder Ihren Räumlichkeiten zu verhindern.
- **Verschließen Sie** Schubladen, Schränke oder Aktenschränke, die sensible Dokumente, Geräte oder Speichermedien enthalten, wenn sie nicht benutzt werden.
- Sichern Sie **Peripheriegeräte** wie Tastaturen, Maus und externe Speichergeräte (USB, Festplatten usw.) und bewahren Sie sie in verschlossenen Schubladen oder Schränken auf.

Co-funded by the European Union

4. Best Practices - Empfehlungen

4.1. Sicheres Umfeld

Cybersicherheit beginnt offline: Bevor Sie technische Schutzmaßnahmen ergreifen, sollten Sie Ihren physischen Raum so organisieren, dass Gefahren und Schwachstellen reduziert werden.

3. Führen Sie eine „Clean-Desk-Regel“ ein

Halten Sie eine **„Clean-Desk-Regel“ ein**, indem Sie sensible Dokumente, Notizen oder Passwörter von Ihrem Schreibtisch entfernen, wenn Sie nicht anwesend sind. Bewahren Sie physische Dokumente sicher auf, vorzugsweise in verschlossenen Schränken oder Schubladen.

Tipp

Eine gute Praxis ist es, einen "0-Papier-Schreibtisch" anzustreben, auf dem nur die Papiere liegen, die gerade benutzt werden. Dies steigert nicht nur nachweislich die Effizienz und verringert den Stress, sondern verringert auch das Risiko, dass wichtige Informationen für Unbefugte sichtbar bleiben.

4. Verwenden Sie Sichtschutzwände

Verwenden Sie **Sichtschutzwände oder Filter** auf Computern oder mobilen Geräten, um zu verhindern, dass Unbefugte Ihren Bildschirm einsehen können. Sichtschutzfilter zwingen die Betrachter, sich genau vor dem Gerät aufzuhalten, und verhindern das "Shoulder-Surfing". Sie sind bei einigen Geräten bereits integriert oder können heruntergeladen werden.

Tipps

- Auf Computern mit integriertem Datenschutzbildschirm drücken Sie F12 oder Fn + D, um ihn zu aktivieren.
- Auf Android sind die am besten bewerteten Datenschutz-Apps 1) Privacy Screen, 2) Screen Guard Privacy, 3) Privacy Filter

4. Best Practices - Empfehlungen

4.1. Sicheres Umfeld

Cybersicherheit beginnt offline: Bevor Sie technische Schutzmaßnahmen ergreifen, sollten Sie Ihren physischen Raum so organisieren, dass Gefahren und Schwachstellen reduziert werden.

5. Vernichten Sie sensible Dokumente

Schreddern oder entsorgen Sie physische Dokumente mit sensiblen Informationen, wie Finanzunterlagen, Personalausweise usw., bevor Sie sie wegwerfen. Werfen Sie sie nicht einfach in den Mülleimer, ohne ein Dokument **zumindest zu zerreißen**.

Tipp

Auch wenn Recycling heute zu den Aufgaben von allen Mitarbeiter:innen gehört, sollte man nicht vergessen, dass loses Papier oft unbeaufsichtigt gelassen wird, bevor es recycelt wird, und dass dies Ihr Unternehmen anfällig für Sicherheitslücken machen kann.

6. Schreiben Sie keine Passwörter auf

Notieren Sie Passwörter oder PINs **nicht** auf Haftnotizen, Notizbüchern oder physischen Dokumenten. Wenn Sie ein Passwort unbedingt aufschreiben müssen, tun Sie dies an einem Ort, an dem es nicht gefunden werden kann, und verschlüsseln Sie es mit einem Code, den nur Sie entziffern können (z. B.: Anzahl der Kinder der Schwester / Geburtstagsmonat des Hundes, usw.)

Tipp

Verwenden Sie stattdessen einen seriösen Passwortmanager, um Ihre Passwörter sicher zu speichern und zu verwalten. Das einzige Passwort, das Sie sich merken müssen, ist das des Passwortmanagers.

Co-funded by the European Union

4. Best Practices - Empfehlungen

4.1. Sicheres Umfeld

Cybersicherheit beginnt offline: Bevor Sie technische Schutzmaßnahmen ergreifen, sollten Sie Ihren physischen Raum so organisieren, dass Gefahren und Schwachstellen reduziert werden.

7. Achten Sie auf das Schulter-Surfen

Achten Sie auf Ihre Umgebung und schützen Sie Ihren Bildschirm und Ihre Tastatur vor den Blicken Unbefugter, insbesondere an öffentlichen Orten. **Schützen Sie Ihre Tastatur**, wenn Sie PINs oder Passwörter an Geldautomaten, Tastaturen oder mobilen Geräten eingeben.

Tipps

- Sichtschutzwände sind ein gutes Mittel gegen das Schulter-Surfen.
- Wenn Sie sich in einem öffentlichen Raum aufhalten, setzen Sie sich am besten mit dem Rücken an eine Wand, um das Surfen von hinten zu vermeiden.

8. Aktivieren der Festplattenverschlüsselung

Aktivieren Sie die **Festplattenverschlüsselung** auf Ihren Geräten, um die auf der Festplatte oder den Speichermedien des Geräts gespeicherten Daten zu schützen. Dadurch wird sichergestellt, dass selbst bei Diebstahl oder Verlust Ihres Geräts unbefugte Benutzer:innen ohne den Verschlüsselungsschlüssel nicht auf die Daten zugreifen können.

Tipps

- Unter Windows aktivieren Sie die Verschlüsselung unter Einstellungen > Datenschutz und Sicherheit
- Die meisten mobilen Betriebssysteme verfügen inzwischen auch über Funktionen, mit denen sich Daten bei Verlust des Geräts aus der Ferne löschen lassen.

Co-funded by the European Union

4. Best Practices - Empfehlungen

4.2. Sicheres Surfen

Achten Sie beim **Surfen** im Internet auf die Einhaltung der folgenden bewährten Praktiken.

1. Verwenden Sie sichere Websites (HTTPS)
2. Updaten Sie Ihre Software und Ihr Betriebssystem
3. Verwenden Sie Werbeblocker und Inhaltsfilter
4. Seien Sie vorsichtig mit Downloads
5. Surfen Sie anonym
6. Löschen Sie regelmäßig Browser-Cache und Cookies

Co-funded by the European Union

4. Best Practices - Empfehlungen

4.2. Sicheres Surfen

Achten Sie beim **Surfen** im Internet auf die Einhaltung der folgenden bewährten Praktiken.

1. Verwenden Sie sichere Websites (HTTPS)

Achten Sie auf **HTTPS** in der URL der Website, um eine sichere Verbindung zu gewährleisten, wenn Sie vertrauliche Daten wie Anmeldedaten oder finanzielle Details übertragen. Vermeiden Sie es, persönliche Daten auf Websites einzugeben, die nur **HTTP** verwenden.

Tipp

HTTP-Nachrichten werden im Klartext übertragen, was bedeutet, dass Unbefugte sie leicht über das Internet abrufen und lesen können. HTTPS überträgt alle Daten in verschlüsselter Form. Wenn Benutzer:innen sensible Daten übermitteln, können keine Dritten die Daten über das Netz abfangen.

2. Updaten Sie Ihre Software und Ihr Betriebssystem

Aktualisieren Sie regelmäßig Ihr Betriebssystem, Ihren Webbrowser, Ihre Antivirensoftware und andere Anwendungen, um bekannte Sicherheitslücken zu schließen und sich vor Sicherheitsbedrohungen zu schützen.

Tipp

Zögern Sie die Aktualisierung aller Software und Anwendungen, die Sie (privat und beruflich) nutzen, nicht hinaus, wenn Sie eine Update-Benachrichtigung erhalten. Vergewissern Sie sich regelmäßig, dass in Ihrem Anwendungszentrum alles auf dem neuesten Stand ist.

Co-funded by the European Union

4. Best Practices - Empfehlungen

4.2. Sicheres Surfen

Achten Sie beim **Surfen** im Internet auf die Einhaltung der folgenden bewährten Praktiken.

3. Verwenden Sie Werbeblocker und Inhaltsfilter

Installieren Sie **Werbeblocker und Inhaltsfilter**, um zu verhindern, dass bösartige Werbung, Pop-ups oder Skripte Ihr Surferlebnis beeinträchtigen oder Malware verbreiten. Bestimmte Websites erfordern möglicherweise eine Deaktivierung, um auf Inhalte zugreifen zu können, was über das Symbol in Ihrem Browser leicht möglich ist.

Tipps

Am besten bewertete kostenlose Adblocker:

- uBlock Herkunft
- Datenschutz Badger
- Ghostery
- Adblock plus

4. Seien Sie vorsichtig mit Downloads

Laden Sie Software, Dateien und Anhänge nur von **seriösen Quellen** herunter und vermeiden Sie das Herunterladen von Inhalten von nicht vertrauenswürdigen Websites oder unbekannten Quellen, um das Risiko einer Malware-Infektion zu minimieren.

Tipp

Im Internet ist eine unglaubliche Menge an Inhalten verfügbar. Wenn Sie auf einer Website etwas herunterladen müssen, können Sie wahrscheinlich auf ähnliche Inhalte auf einer anderen Website zugreifen, ohne etwas herunterladen zu müssen.

Co-funded by the European Union

4. Best Practices - Empfehlungen

4.2. Sicheres Surfen

Achten Sie beim **Surfen** im Internet auf die Einhaltung der folgenden bewährten Praktiken.

5. Anonym surfen

Ziehen Sie die Nutzung eines **virtuellen privaten Netzwerks (VPN) in** Betracht, um Ihren Internetverkehr **zu verschlüsseln** und anonym zu surfen, insbesondere bei der Nutzung öffentlicher Wi-Fi-Netzwerke oder beim Zugriff auf sensible Informationen.

Tipp

Verwechseln Sie den "Inkognito"-Modus oder den "Private Browsing"-Modus nicht mit einem VPN: Sie machen Ihr Surfen nicht sicherer, sondern löschen lediglich Ihren Browserverlauf von Ihrem Gerät. Aber Ihr Browserverlauf ist immer noch für die Außenwelt sichtbar, ebenso wie Ihre IP-Adresse, Ihr Netzwerk usw.

6. Regelmäßig Browser-Cache und Cookies löschen

Löschen Sie regelmäßig Ihren Browser-Cache, Ihre Cookies und Ihren Browserverlauf, um **Tracking-Daten zu** entfernen und das Risiko eines unbefugten Zugriffs auf Ihre Surfgewohnheiten oder persönlichen Daten zu minimieren.

Tipp

Klicken Sie in Chrome auf die 3 Punkte in der oberen rechten Ecke > Browserdaten löschen. Wählen Sie in der neu geöffneten Registerkarte den Zeitraum aus, für den Sie Daten löschen möchten (idealerweise "Alle Zeit"), wählen Sie die drei Optionen (Browserverlauf, Cookies und Cache) und klicken Sie auf "Browserdaten löschen", um Ihren Browser sofort zu löschen.

4. Best Practices - Empfehlungen

4.3. Sicherer E-Mail-Versand

Wenn Sie eine E-Mail erhalten, sollten Sie sich die folgenden Fragen stellen, um Sicherheitsprobleme zu vermeiden:

1. Kenne und erkenne ich Absender/Absenderin?
2. Ist die E-Mail unerwartet oder unaufgefordert?
3. Bin ich in der E-Mail mit meinem Namen angesprochen?
4. Gibt es Rechtschreib- oder Grammatikfehler?
5. Gibt es verdächtige Anhänge?
6. Enthält die E-Mail unerwartete Links?
7. Wird in der E-Mail nach vertraulichen Informationen gefragt?
8. Sehen die Unterschrift und die Kontaktinformationen echt aus?
9. Besteht eine Beziehung zwischen mir und dem Absender/der Absenderin?
10. Wird in der E-Mail mit Drohungen oder Angstmache gearbeitet?
11. Hat das Antivirenprogramm etwas Verdächtiges entdeckt?
12. Sieht sie aus wie andere E-Mails von diesem Anbieter:innen?

Co-funded by the European Union

4. Best Practices - Empfehlungen

4.3. Sicherer E-Mail-Versand

Wenn Sie eine E-Mail erhalten, sollten Sie sich die folgenden Fragen stellen, um Sicherheitsprobleme zu vermeiden:

Achten Sie außerdem darauf, dass Sie eine E-Mail immer mit der folgenden **Einstellung** behandeln:

- **Niemals sofortige, überstürzte Maßnahmen ergreifen**
- **Gehen Sie immer davon aus, dass es sich** bei einer E-Mail um einen **Betrug** handeln könnte, und nehmen Sie sich die Zeit, sie zu studieren und zu "löschen".
- **Vertrauen Sie auf Ihr Urteilsvermögen** und Ihren Instinkt: Wenn Ihnen etwas komisch vorkommt, sollten Sie es mit Vorsicht erkunden.
- Denken Sie daran, dass Betrüger mit **Gefühlen** wie Angst, Einschüchterung und Drohungen spielen. Behalten Sie einen **kühlen Kopf** und bleiben Sie in jedem Fall **ruhig**.

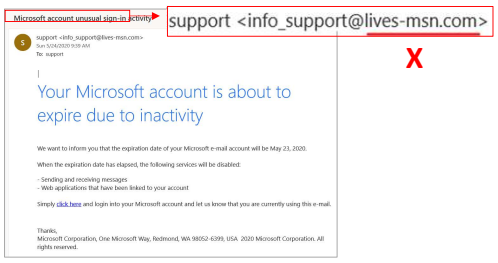
4. Best Practices - Empfehlungen

4.3. Sicherer E-Mail-Versand

Wenn Sie eine E-Mail erhalten, sollten Sie sich die folgenden Fragen stellen, um Sicherheitsprobleme zu vermeiden:

1. Kenne und erkenne ich den Absender/die Absenderin?

Überprüfen Sie die Identität des Absenders/der Absenderin, indem Sie nicht nur den oben und in der Signatur angezeigten Namen, sondern auch die **tatsächliche E-Mail-Adresse**, von der die E-Mail gesendet wurde, betrachten.



X

2. Ist die E-Mail unerwartet oder unaufgefordert?

Seien Sie vorsichtig mit unerwarteten E-Mails, insbesondere mit solchen, in denen **dringende Maßnahmen** gefordert oder **unaufgeforderte Dienstleistungen** angeboten werden. Betrüger nutzen sie oft, um die Empfänger auszutricksen, am häufigsten mit diesen Themen:

- Kontoinformationen müssen aktualisiert oder überprüft werden (Kontosperrung, Ablauf, Sicherheitswarnung, usw.)
- Sie möchten eine ausstehende Rechnung über einen Link bezahlen
- Angebote von gefälschten Arbeitsangeboten
- Zahlung oder Fernzugriff auf den Computer oder das Konto, der vom "Support" beantragt wird, um technische Probleme zu lösen.
- Sie müssen Bearbeitungsgebühren zahlen oder persönliche Daten angeben, um eine unaufgeforderte Belohnung oder einen Preis zu erhalten.

Co-funded by the European Union

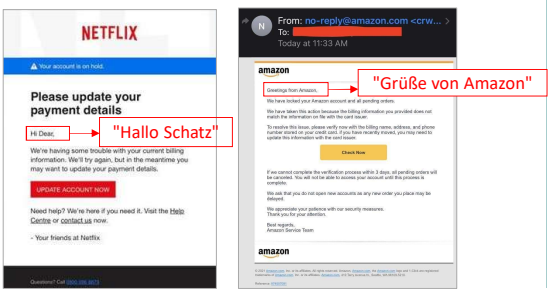
4. Best Practices - Empfehlungen

4.3. Sicherer E-Mail-Versand

Wenn Sie eine E-Mail erhalten, sollten Sie sich die folgenden Fragen stellen, um Sicherheitsprobleme zu vermeiden:

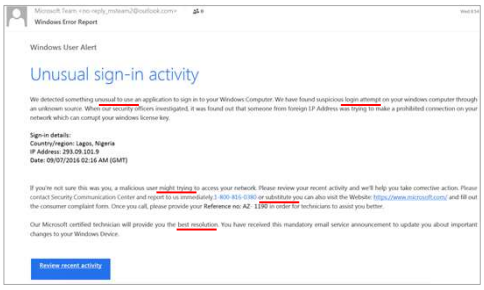
3. Bin ich in der E-Mail mit meinem Namen angesprochen?

Seriöse Organisationen verwenden oft Ihren Namen in ihren Mitteilungen. **Allgemeine Begrüßungen** oder **falsche Schreibweisen** Ihres Namens können ein Warnsignal sein.



4. Gibt es Rechtschreib- oder Grammatikfehler?

Schlecht geschriebene E-Mails mit Rechtschreib- oder **Grammatikfehlern** können auf einen Phishing-Versuch hindeuten. Seriöse Unternehmen machen in der Regel weniger Fehler in ihren E-Mails.



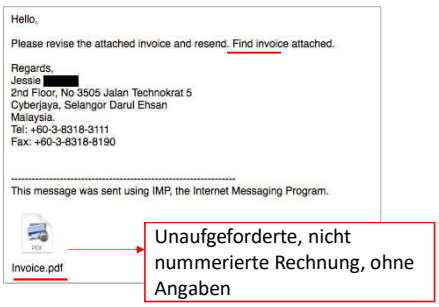
4. Best Practices - Empfehlungen

4.3. Sicherer E-Mail-Versand

Wenn Sie eine E-Mail erhalten, sollten Sie sich die folgenden Fragen stellen, um Sicherheitsprobleme zu vermeiden:

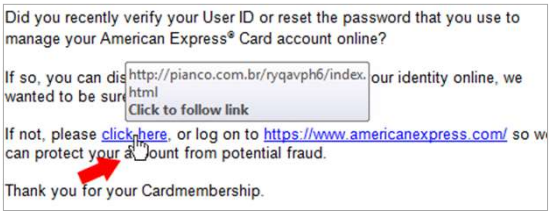
5. Gibt es verdächtige Anhänge?

Vermeiden Sie es, **unerwartete Anhänge** zu öffnen, insbesondere von unbekannten Quellen. Bösartige Anhänge können **Malware** oder Phishing-Versuche enthalten.



6. Enthält die E-Mail unerwartete Links?

Bewegen Sie den Mauszeiger über einen Link in der E-Mail, ohne ihn anzuklicken, um die **tatsächliche URL** zu sehen. Wenn der Link nicht mit der offiziellen Website des angeblichen Absenders übereinstimmt oder verdächtig aussieht, könnte es sich um einen Phishing-Versuch handeln.



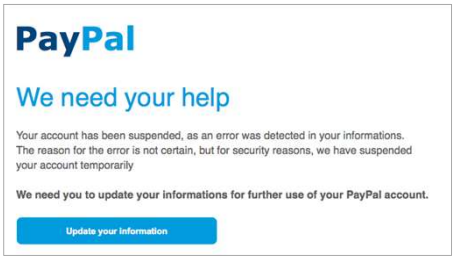
4. Best Practices - Empfehlungen

4.3. Sicherer E-Mail-Versand

Wenn Sie eine E-Mail erhalten, sollten Sie sich die folgenden Fragen stellen, um Sicherheitsprobleme zu vermeiden:

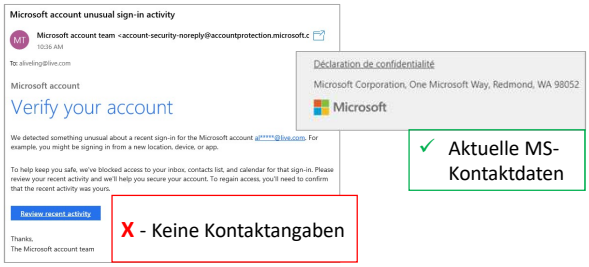
7. Wird nach vertraulichen Informationen gefragt?

Unternehmen **fordern** normalerweise **keine sensiblen Daten** per **E-Mail** oder über einen **Link an** (z. B. Passwörter oder Kreditkartendaten), sondern fordern Sie normalerweise auf, sich auf ihrer Website mit **Ihrem Konto zu** verbinden.



8. Sehen Unterschrift und Kontaktinformationen echt aus?

Seriöse Organisationen geben in ihren E-Mails in der Regel **eindeutige Kontaktinformationen an**, einschließlich einer **physischen Adresse**. Überprüfen Sie die Angaben des Absenders, einschließlich seiner **Unterschrift,** und vergleichen Sie sie mit offiziellen Quellen.



✓ Aktuelle MS-Kontaktdaten

X - Keine Kontaktangaben

JIHOMĚSTSKÁ SOCIÁLNÍ a.s. · MPA · MedicalCare · ápenhet · Co-funded by the European Union

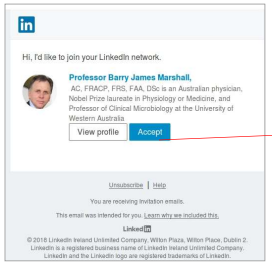
4. Best Practices - Empfehlungen

4.3. Sicherer E-Mail-Versand

Wenn Sie eine E-Mail erhalten, sollten Sie sich die folgenden Fragen stellen, um Sicherheitsprobleme zu vermeiden:

9. Besteht eine Beziehung zwischen mir und dem Absender/der Absenderin?

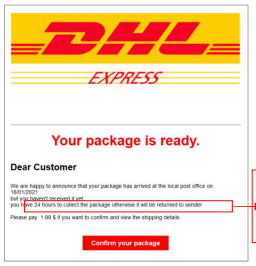
Wenn die E-Mail behauptet, von einer Organisation zu stammen, bei der Sie ein Konto haben, überprüfen Sie die Informationen **in Ihrem Konto**, anstatt sich nur auf eine E-Mail zu verlassen.



Überprüfen Sie Ihr LinkedIn-Konto, anstatt auf "Akzeptieren" zu klicken.

10. Wird mit Drohungen/Angstmache gearbeitet?

Betrüger:innen verwenden **Drohungen**, **Einschüchterungen** oder Angsttaktiken, um Empfänger:innen zum schnellen Handeln zu bewegen. Seien Sie vorsichtig bei E-Mails, die ein Gefühl von **Dringlichkeit** oder **Angst vermitteln**.



"Sie haben 24 Stunden Zeit, das Paket abzuholen, sonst wird es an den Absender zurückgeschickt.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s. · MPA · MedicalCare · ápenhet · Co-funded by the European Union

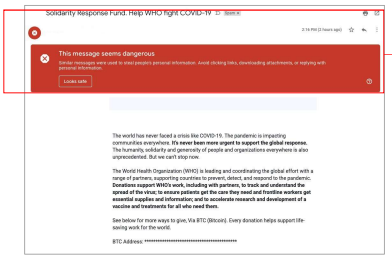
4. Best Practices - Empfehlungen

4.3. Sicherer E-Mail-Versand

Wenn Sie eine E-Mail erhalten, sollten Sie sich die folgenden Fragen stellen, um Sicherheitsprobleme zu vermeiden:

11. Hat das Antivirenprogramm Verdächtiges entdeckt?

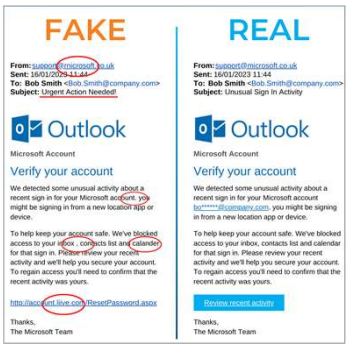
Die meisten E-Mail-Anbieter verfügen über **integrierte Module zur** Erkennung von Phishing-Versuchen. Außerdem könnte Ihr eigenes **Antivirenprogramm** die E-Mail als **verdächtig** eingestuft haben. Wenn dies der Fall ist, sollten Sie mit der E-Mail **vorsichtig** umgehen.



"Diese Nachricht scheint gefährlich zu sein"

12. Sieht sie aus wie andere E-Mails von diesem Anbieter?

Wenn Sie eine E-Mail von einer Organisation erhalten, von der Sie **bereits E-Mails erhalten haben**, überprüfen Sie, ob das Design, das Branding, die Kontaktdaten, das Copyright, die Links und die Sprache **übereinstimmen**, bevor Sie der E-Mail vertrauen.



JIHOMĚSTSKÁ SOCIÁLNÍ a.s. | MPA | MedicalCare | åpenhet | Co-funded by the European Union

4. Best Practices - Empfehlungen

4.4. Sichere Nutzung sozialer Medien

Nutzen Sie soziale Medien sicher, indem Sie die Folgendes berücksichtigen

1. Überprüfen und Anpassen der Datenschutzeinstellungen
2. Seien Sie selektiv bei Freundschaftsanfragen und Verbindungen
3. Vorsicht vor Phishing und Betrug
4. Achten Sie auf die Freigabe von Standorten und auf das, was Sie veröffentlichen
5. Überprüfen Sie die Authentizität Ihres Kontos
6. Kontrollieren Sie Drittanbieteranwendungen und -berechtigungen

JIHOMĚSTSKÁ SOCIÁLNÍ a.s. | MPA | MedicalCare | åpenhet | Co-funded by the European Union

4. Best Practices - Empfehlungen

4.4. Soziale Medien und Nachrichtenübermittlung

Nutzen Sie soziale Medien sicher, indem Sie die Folgendes berücksichtigen

1. Überprüfen und Anpassen der Datenschutzeinstellungen

Überprüfen Sie regelmäßig **Ihre Datenschutzeinstellungen** auf sozialen Medienplattformen **und passen Sie diese an**, um zu kontrollieren, wer Ihre Beiträge, persönlichen Informationen und Fotos sehen kann.
Schränken Sie die Zielgruppe für Ihre Beiträge **ein** und überlegen Sie, ob Sie **den Zugang** zu sensiblen Informationen auf vertrauenswürdige Freunde und Kontakte beschränken wollen.

Tipp

Die meisten Standard-Datenschutzeinstellungen in sozialen Medien können die Weitergabe Ihrer Daten an andere Online-Nutzer erlauben, einschließlich Ihres Namens, Alters, Wohnorts, Geschlechts usw.

2. Seien Sie selektiv bei Freundschaftsanfragen und Verbindungen

Seien Sie vorsichtig, wenn Sie **Freundschaftsanfragen oder Verbindungen** von unbekannten Personen annehmen. Überprüfen Sie die Identität der Person, bevor Sie ihre Anfrage annehmen, insbesondere wenn Sie sie nicht persönlich kennen. Viele Social-Media-Betrügereien beginnen damit, "Ihr Freund" zu werden und **auf mehr Ihrer Daten zuzugreifen**.

Tipp

Versuchen Sie, die Echtheit der Anfrage mit anderen Mitteln zu überprüfen. Beispiel: Wenn Sie eine Anfrage von jemandem erhalten, der behauptet, der Bruder Ihres Freundes zu sein, können Sie Ihren Freund bitten, die Identität der Person zu bestätigen, bevor Sie sie annehmen.

Co-funded by the European Union

4. Best Practices - Empfehlungen

4.4. Soziale Medien und Nachrichtenübermittlung

Nutzen Sie soziale Medien sicher, indem Sie die Folgendes berücksichtigen

3. Hüten Sie sich vor Phishing und Betrug

Seien Sie **vorsichtig bei unaufgeforderten** Nachrichten, Links oder Anfragen von unbekannten Personen in sozialen Medien. **Vermeiden Sie es, auf verdächtige Links zu klicken** oder Anhänge von unbekannten Quellen herunterzuladen, da diese zu Phishing-Betrug oder Malware-Infektionen führen können.

Tipp

Viele Social-Media-Betrügereien geschehen durch das Hacken des Kontos eines Ihrer Kontakte. Seien Sie vorsichtig, wenn ein Ihnen bekannter Kontakt Ihnen unaufgeforderte, ungewöhnliche Anfragen sendet (z. B. finanzielle Unterstützung für seine Verwandten im Krankenhaus), und überprüfen Sie diese über ein anderes Medium.)

4. Achten Sie auf die Freigabe von Standorten und darauf, was Sie posten

Schränken Sie die Weitergabe Ihres Standorts auf sozialen Medienplattformen **ein**, insbesondere wenn Sie Fotos oder Updates in Echtzeit posten. Vermeiden Sie es, Ihren genauen Standort preiszugeben oder persönliche Informationen zu teilen, die Ihre Sicherheit gefährden könnten.

Tipp

Viele Arten von Informationen können von Cyberkriminellen genutzt werden, um Schaden anzurichten. Abgesehen von den offensichtlichen Informationen (Name, Alter, Geschlecht, Wohnort usw.) können Cyberkriminelle viele Details nutzen, z. B. den Namen der nächstgelegenen Schule, den früheren oder aktuellen Arbeitsplatz, Screenshots mit persönlichen Daten usw.

Co-funded by the European Union

4. Best Practices - Empfehlungen

4.4. Soziale Medien und Nachrichtenübermittlung

Nutzen Sie soziale Medien sicher, indem Sie die Folgendes berücksichtigen

5. Überprüfung der Authentizität Ihres Kontos

Seien Sie misstrauisch gegenüber **gefälschten oder nachgemachten Konten** auf Social-Media-Plattformen, insbesondere solchen, die sich als Prominente, öffentliche Personen oder Marken ausgeben. **Überprüfen Sie die Authentizität** von Konten, bevor Sie mit ihnen interagieren oder persönliche Informationen weitergeben.

Tipp

Allein im Jahr 2021 entfernte Facebook 1,7 Milliarden gefälschte Konten. Ebenso sind fast 1 von 5 (19,42 %) Twitter-Handles gefälscht oder Spam. Das blaue Häkchen, mit dem ein Konto "zertifiziert" wird, kann von praktisch jedem erworben werden und ist kein Indikator dafür, dass einem Konto vertraut werden kann.

6. Überwachen Sie Anwendungen von Drittanbietern und deren Berechtigungen

Überprüfen und verwalten Sie regelmäßig die Berechtigungen für Drittanbieter-Apps, die mit Ihren Social-Media-Konten verbunden sind. Entfernen Sie den Zugriff für Apps, die Sie nicht mehr verwenden oder denen Sie nicht mehr vertrauen, um das Risiko von Datenmissbrauch oder Datenschutzverletzungen zu minimieren.

Tipp

Achten Sie auf die Berechtigungen, die Sie diesen Anwendungen erteilen, denn sie könnten Zugang zu privaten Informationen gewähren, in die sie nicht eingeweiht sein sollten.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s. · MWA · MedicalCare · åpenhet · Co-funded by the European Union

4. Best Practices - Empfehlungen

4.5. Sicherheit mobiler Geräte

Nutzen Sie Ihr **mobiles Gerät sicherer**, indem Sie Folgendes berücksichtigen.

1. Verwenden Sie eine sichere Bildschirmsperre
2. Halten Sie Ihre Software und Ihr Betriebssystem auf dem neuesten Stand
3. Daten verschlüsseln
4. Verwenden Sie einen vertrauenswürdigen App-Store
5. App-Berechtigungen überprüfen
6. Seien Sie vorsichtig bei öffentlichem WiFi
7. Aktivieren Sie "Mein Gerät suchen"
8. Beschränken Sie die Verwendung von Bluetooth und NFC

JIHOMĚSTSKÁ SOCIÁLNÍ a.s. · MWA · MedicalCare · åpenhet · Co-funded by the European Union

4. Best Practices - Empfehlungen

4.5. Sicherheit mobiler Geräte

Nutzen Sie Ihr **mobiles Gerät sicherer**, indem Sie Folgendes berücksichtigen.

1. Verwenden Sie eine sichere Bildschirmsperre

Aktivieren Sie eine **sichere Bildschirmsperre** (z. B. PIN, Kennwort, Muster, biometrische Identifizierung), um unbefugten Zugriff auf Ihr Gerät zu verhindern, wenn es verloren geht oder gestohlen wird. Vermeiden Sie die Verwendung leicht zu erratender Muster oder PINs.

2. Halten Sie Ihre Software und Ihr Betriebssystem auf dem neuesten Stand

Aktualisieren Sie regelmäßig **Ihr mobiles Betriebssystem**, Ihre Anwendungen und Sicherheitspatches, um sich vor bekannten Schwachstellen und Sicherheitsbedrohungen zu schützen. Aktivieren Sie automatische Updates, um rechtzeitige Sicherheitspatches zu gewährleisten.

3. Daten verschlüsseln

Aktivieren Sie die Verschlüsselung der auf Ihrem mobilen Gerät gespeicherten Daten, um sensible Informationen zu schützen. Die meisten modernen Mobilgeräte bieten integrierte Verschlüsselungsfunktionen, die Daten im Ruhezustand verschlüsseln.

4. Verwenden Sie einen vertrauenswürdigen App-Store

Laden Sie Apps nur aus **offiziellen und vertrauenswürdigen App-Stores** wie dem Apple App Store oder dem Google Play Store herunter, um das Risiko des Herunterladens von bösartigen Apps oder Malware zu minimieren.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s. MPA MedicalCare åpenhet Co-funded by the European Union

4. Best Practices - Empfehlungen

4.5. Sicherheit mobiler Geräte

Nutzen Sie Ihr **mobiles Gerät sicherer**, indem Sie Folgendes berücksichtigen.

5. App-Berechtigungen überprüfen

Überprüfen und verwalten Sie App-Berechtigungen, um zu kontrollieren, auf welche Daten und Funktionen Apps auf Ihrem Gerät zugreifen können. **Deaktivieren Sie unnötige Berechtigungen**, die Apps für ihre Funktionalität nicht benötigen.

6. Seien Sie vorsichtig bei öffentlichem WiFi

Vermeiden Sie es, sich mit **ungesicherten öffentlichen WiFi-Netzwerken** zu verbinden, da diese anfällig für Abhör- oder Man-in-the-Middle-Angriffe sein können. **Verwenden Sie ein VPN**, um Ihren Internetverkehr zu verschlüsseln, wenn Sie sich mit öffentlichen WLAN-Netzwerken verbinden.

7. Aktivieren Sie "Mein Gerät suchen".

Aktivieren Sie die Funktion "**Mein Gerät suchen**" oder "**Mein iPhone suchen**" auf Ihrem Mobilgerät, um Ihr Gerät aus der Ferne zu orten, zu sperren oder zu löschen, falls es verloren geht oder gestohlen wird. Diese Funktion hilft, Ihre Daten und Ihre Privatsphäre im Falle eines Diebstahls oder Verlusts zu schützen.

8. Beschränken Sie die Nutzung von Bluetooth und NFC

Deaktivieren Sie Bluetooth und NFC, wenn Sie es nicht benutzen, um unbefugten Zugriff oder Kopplung mit anderen Geräten zu verhindern. Seien Sie beim Pairing mit unbekannten Geräten vorsichtig und verwenden Sie Bluetooth-Geräte aus vertrauenswürdigen Quellen.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s. MPA MedicalCare åpenhet Co-funded by the European Union

4. Best Practices - Empfehlungen

4.6. Passwortsicherheit

Sichern Sie Ihre Passwörter ab, indem Sie Folgendes sicherstellen.

1. Verwenden Sie sichere und eindeutige Passwörter
2. Verwenden Sie unterschiedliche Passwörter für jedes Konto
3. Verwenden Sie Passphrasen anstelle von Wörtern
4. Verwenden Sie einen seriösen Passwort-Manager
5. Behandeln Sie Ihre Passwörter immer vertraulich
6. Aktualisieren Sie Ihre Passwörter regelmäßig

4. Best Practices - Empfehlungen

4.6. Passwortsicherheit

Sichern Sie Ihre Passwörter ab, indem Sie Folgendes sicherstellen.

1. Verwenden Sie sichere und eindeutige Passwörter

Erstellen Sie starke, komplexe Passwörter, die schwer zu erraten sind. Verwenden Sie eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Vermeiden Sie leicht zu erratende Informationen wie Namen, Geburtstage oder gängige Wörter.

Tipps

Einige Websites geben Ihnen einen Hinweis auf die Sicherheit Ihres Passworts. Registrieren Sie kein Passwort, bevor es nicht von der Website oder Software als "sicher" eingestuft wurde. Passwörter sollten aus mindestens 16 Zeichen bestehen und verschiedene Arten von Zeichen enthalten.

2. Verwenden Sie unterschiedliche Passwörter für jedes Konto

Verwenden Sie nicht dasselbe Passwort für mehrere Konten. Verwenden Sie für jedes Online-Konto ein eindeutiges Passwort, um die Auswirkungen einer Sicherheitsverletzung auf andere Konten zu minimieren.

Tipp

Verwenden Sie einen Passwort-Manager, damit Sie sich keine Passwörter merken oder aufschreiben müssen. Sie müssen sich nur noch das Passwort für Ihren Passwortmanager merken.

Co-funded by the European Union

4. Best Practices - Empfehlungen

4.6. Passwortsicherheit

Sichern Sie Ihre Passwörter ab, indem Sie Folgendes sicherstellen.

3. Verwenden Sie Passphrasen anstelle von Wörtern

Erwägen Sie die Verwendung von **Passphrasen** anstelle von herkömmlichen Passwörtern. Passphrasen sind längere **Kombinationen von Wörtern oder Sätzen**, die leichter zu merken, aber schwerer zu knacken sind. Zum Beispiel ist "Icàre@b0utSecur1ty!" eine starke Passphrase.

Tipp

Wählen Sie zunächst eine Passphrase, die Sie sich leicht merken können. Legen Sie dann Ihr eigenes "Verschlüsselungssystem" fest, z.B.: o=0, i=1, a=@, usw. Achten Sie darauf, auch Großbuchstaben und Sonderzeichen zu integrieren.

4. Verwenden Sie einen seriösen Passwort-Manager

Verwenden Sie einen **seriösen Passwortmanager**, um Ihre Passwörter sicher zu speichern und zu verwalten. Passwort-Manager generieren starke, eindeutige Passwörter für jedes Konto und speichern sie in einem verschlüsselten Tresor, der nur mit einem Master-Passwort zugänglich ist.

Tipps

Beispiele für seriöse Passwortmanager finden Sie im letzten Abschnitt dieses Curriculums. Stellen Sie sicher, dass Sie die Funktion zur Generierung von Passwörtern nutzen, um von einzigartigen, sicheren und zufällig generierten Passwörtern zu profitieren, die Sie sich nicht merken müssen.

Co-funded by the European Union

4. Best Practices - Empfehlungen

4.6. Passwortsicherheit

Sichern Sie Ihre Passwörter ab, indem Sie Folgendes sicherstellen.

5. Behandeln Sie Ihre Passwörter immer vertraulich

Geben Sie Ihre Passwörter niemals an andere weiter, auch nicht an Freunde, Familienmitglieder oder Kollegen. Halten Sie Ihre Passwörter vertraulich und vermeiden Sie es, sie aufzuschreiben oder an leicht zugänglichen Orten aufzubewahren. Achten Sie darauf, sie in einem Passwort-Manager zu speichern.

Tipps

Wenn die Weitergabe eines Passworts unvermeidlich ist, tun Sie dies am besten mündlich oder alternativ über eine sichere, verschlüsselte Anwendung (z. B. niemals über einen Nachrichtenkanal in den sozialen Medien). Teilen Sie niemals die Login-/E-Mail-Adresse über dieselbe Anwendung, sondern über ein anderes Medium.

6. Aktualisieren Sie Ihre Passwörter regelmäßig

Aktualisieren Sie regelmäßig Ihre Passwörter für Online-Konten, insbesondere für sensible Konten wie Bankkonten, E-Mail-Konten oder Konten in sozialen Medien. Ändern Sie Passwörter sofort, wenn Sie den Verdacht haben, dass sie kompromittiert wurden, und lassen Sie den Passwortmanager regelmäßig neue Passwörter generieren.

Tipp

Denken Sie daran, die Standardkennwörter von Geräten, Routern oder Softwareanwendungen zu ändern. Standardpasswörter sind oft leicht zu erraten und weithin bekannt, was sie anfällig für unbefugten Zugriff macht.

Co-funded by the European Union

5. Nützliche Tools und zusätzliche Ressourcen

1. Passwort-Manager
2. 2FA-Tools
3. Anti-Malware
4. Verschlüsselungs-Tools
5. Weitere Tools

Co-funded by the European Union

5. Nützliche Tools und zusätzliche Ressourcen

5.1. Passwort-Manager

LastPass 1Password NordPass KEEPER

Passwort-Manager **speichern und verwalten Passwörter sicher** für verschiedene Konten und vereinfachen den Zugang, während sie gleichzeitig die Erstellung starker, eindeutiger Passwörter und einen sicheren Zugang gewährleisten. Stellen Sie das sicher:

- **Wählen Sie ein starkes, einzigartiges und einprägsames Master-Passwort**, mit dem Sie Zugang zum Passwort-Manager erhalten. Vergessen Sie es nicht und geben Sie es niemals weiter; es ist die Tür zu all Ihren Konten.
- **Lassen Sie den Passwort-Manager sichere, eindeutige Passwörter** für jedes Ihrer Konten **erstellen**. Er merkt sie sich und speichert sie, so dass Sie nie zweimal dasselbe Passwort haben.

Co-funded by the European Union

5. Nützliche Tools und zusätzliche Ressourcen

5.2. Tools für die Zwei-Faktor-Authentifizierung (2FA)

Tools zur Zwei-Faktor-Authentifizierung (2FA) erhöhen die Sicherheit eines Kontos, indem sie den Benutzer:innen zwingen, seine Anmeldung auf zwei verschiedenen, registrierten und vertrauenswürdigen Geräten zu bestätigen, in der Regel auf dem Telefon und dem Computer.

5. Nützliche Tools und zusätzliche Ressourcen

5.3. Anti-Malware

Anti-Malware oder Anti-Viren identifizieren und entfernen verschiedene Arten von Malware und bieten Echtzeitschutz vor Cyber-Bedrohungen für Geräte und Netzwerke.

5. Nützliche Tools und zusätzliche Ressourcen

5.4. Verschlüsselungs-Tools

Verschlüsselungstools erstellen verschlüsselte Container, die sensible Dateien und Ordner schützen, indem sie unbefugten Zugriff durch Verschlüsselung verhindern. Einige Tools, wie z. B. Bitlocker, verschlüsseln externe Peripheriegeräte wie Festplatten, um deren Sicherheit zu erhöhen.

5. Nützliche Tools und zusätzliche Ressourcen

5.5. Weitere nützliche Tools

Name	Typ	Beschreibung
Daten-schutz Badger	Browser-Erweiterung	Privacy Badger blockiert Tracking-Cookies und Werbung und schützt so die Privatsphäre von Nutzer:innen, indem es verhindert, dass Tracker von Drittanbietern Browsing-Daten sammeln.
Imprivata	Zugangsverwaltung	Imprivata bietet Single-Sign-On-Lösungen an, die es Pflegekräften ermöglichen, mit einem einzigen Login sicher auf mehrere Anwendungen zuzugreifen und so den Workflow zu optimieren, ohne die Sicherheit zu beeinträchtigen.
HIPAA Eins	Tool zur Einhaltung der Vorschriften	HIPAA EINS automatisiert die Einhaltung des HIPAA und unterstützt Organisationen des Gesundheitswesens bei der Erfüllung gesetzlicher Anforderungen, der Durchführung von Risikobewertungen und der Gewährleistung der Datensicherheit.

5. Nützliche Tools und zusätzliche Ressourcen

5.5. Weitere nützliche Tools

Name	Typ	Beschreibung
Symantec Endpoint Protection	Endpunktsicherheit	Symantec Endpoint Protection bietet umfassende Sicherheit, einschließlich fortschrittlichem Schutz vor Bedrohungen, Virenschutz und Firewall-Funktionen, und schützt so vor Cyber-Bedrohungen in Gesundheitsumgebungen.
TeamViewer	Fernzugriff auf den Desktop	TeamViewer ermöglicht den Fernzugriff und die Fernsteuerung von Geräten und unterstützt so den technischen Fernsupport, die Fehlerbehebung und die standortübergreifende Zusammenarbeit.
Cisco AnyConnect	VPN-Werkzeug	Cisco AnyConnect bietet sichere VPN-Verbindungen, die den verschlüsselten Zugriff auf Unternehmensnetzwerke von entfernten Standorten aus ermöglichen und die Datenübertragung schützen.
Adobe Sign	E-Signatur-Plattform	Adobe Sign ermöglicht die sichere digitale Unterzeichnung von Dokumenten, vereinfacht und beschleunigt den Unterzeichnungsprozess und gewährleistet die Einhaltung von Vorschriften und Sicherheit bei der Dokumentenverwaltung.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s. MWA MedicalCare åpenhet Co-funded by the European Union

Vielen Dank für Ihre Teilnahme und Ihre Ideen!

JIHOMĚSTSKÁ SOCIÁLNÍ a.s. MWA MedicalCare åpenhet Co-funded by the European Union