Interreg AUSTRIA–HUNGARY

Co-funded by the European Union

DigiUp NEXT
A COMPETENT BORDER REGION

BERUFSORIENTIERUNGSKONZEPT

CYBER-SICHERHEITSPEZIALIST:IN

Erstellt im Rahmen des Projekts DigiUp NEXT (Aktivität 2.3)

Erstellt von: Sekem Energy / Im Auftrag des BFI Burgenland

März 2026

Das Projekt wird im Rahmen des Programms INTERREG VI-A Österreich-Ungarn 2021-2027 durchgeführt

INHALTSVERZEICHNIS

EINLEITUNG 4

Lernziele 6

DER BERUF – „CYBER SECURITY PROFESSIONAL“ 7

Beschäftigungsmöglichkeiten 7

- Ausbildung & Qualifizierungswege (Österreich) 8
- Beruflicher Einstieg über Lehre 8
- Schulische Ausbildungswege 9
- Höhere Ausbildung (FH & Universität) 9
- Zusatzqualifikationen & Zertifizierungen 10

Cyber-Sicherheitsspezialist:in – mögliche Qualifizierungskette 10

Berufliche Kompetenzen 10

Was macht ein/e Cyber-Sicherheitsspezialist:in konkret? 11

WORKSHOP-EINSTIEG – HACKER ODER BESCHÜTZER? 12

Einstieg 12

SICHERE PASSWÖRTER 14

Ziel 14

Einstieg 14

Hauptteil – Die Passwort-Challenge 15

Präsentation & Bewertung 15

Fachinput – Wie knacken Hacker Passwörter? 16

PHISHING 17

Ziele 17

Beispiele 18

Die 10 wichtigsten Warnsignale 23

Abschluss-Reflexion 23

„WIE HACKBAR IST EIN SCHUL-TAG?“ 24

Ziele 24

Gruppenarbeit - Auftrag 24
Gruppenarbeit - Gruppenphase 25

VR UND AR INHALTE 27
VR-Training: Fehleranalyse in einer IT-Infrastruktur 27

ANHANG: „WIE HACKBAR IST EIN SCHUL-TAG?“ 28

EINLEITUNG

Die digitale Transformation verändert alle Wirtschafts- und Lebensbereiche und führt zu einem tiefgreifenden Wandel der Arbeitswelt. Klassische Berufsbilder entwickeln sich weiter oder verschwinden ganz, während neue Tätigkeitsfelder – insbesondere im IT-Bereich – rasant an Bedeutung gewinnen. Nahezu jede Branche in Österreich – von Industrie und Verwaltung über Handel bis hin zum Gesundheitswesen – ist heute auf digitale Infrastrukturen, automatisierte Prozesse und sichere IT-Systeme angewiesen.

Ein besonders wachsender Bereich ist die Cybersicherheit. Durch die zunehmende Digitalisierung von Unternehmen, Behörden, Schulen und Gesundheitseinrichtungen entstehen immer mehr digitale Angriffsflächen. Gleichzeitig nimmt die Zahl von Cyberangriffen in Österreich kontinuierlich zu. Fachkräfte im Bereich IT-Security zählen daher zu den wichtigsten Zukunftsberufen und gehören zudem zu den bestbezahlten und vielfältigsten Karrierewegen in der IT-Branche. Auch in Befragungen von Jugendlichen zeigt sich, dass finanzielle Sicherheit und attraktive Gehälter eine bedeutende Rolle bei der Berufswahl spielen.

Für Jugendliche zwischen 13 und 16 Jahren eröffnen diese Entwicklungen neue Perspektiven. Viele interessieren sich bereits für digitale Themen wie Programmierung, Computersicherheit, Gaming oder Künstliche Intelligenz, wissen aber oft nicht, welche beruflichen Möglichkeiten dahinterstehen und wie diese Tätigkeiten im Alltag aussehen.

Das Projekt DigiUp Next, durchgeführt im Rahmen des Kooperationsprogramms INTERREG VI-A Österreich–Ungarn, hat deshalb das Ziel, die digitalen Fertigkeiten dieser Altersgruppe zu stärken und die Attraktivität von IT-Berufen zu erhöhen. Grundlage dafür bildet eine empirische Untersuchung mit 1.200 Schülerinnen und Schülern aus beiden Ländern. Die Erhebung zeigte, welche Einstellungen Jugendliche zu IT-Berufen haben, wie sie ihre digitalen Fähigkeiten einschätzen, wie groß ihre Bereitschaft zur Weiterbildung ist und welche Informationsquellen sie im Berufsorientierungsprozess nutzen.

Die Ergebnisse verdeutlichen, dass digitale Geräte – besonders das Smartphone – eine zentrale Rolle im Alltag der Jugendlichen spielen. Zudem zeigte sich ein länderspezifischer Unterschied: Während Jugendliche in Ungarn digitale Technologien stärker für schulische Lernprozesse nutzen, verwenden österreichische Jugendliche digitale Anwendungen häufiger im Freizeit- und Spielbereich. Gleichzeitig ist der Anteil der Jugendlichen, die bereits mit fortgeschrittenen Anwendungen wie Robotik, 3D-Druck oder Programmierung arbeiten, noch gering. Das verweist auf einen deutlichen Förderbedarf im Bereich digitaler Kompetenzen.

Gerade vor diesem Hintergrund wird die Entwicklung zeitgemäßer Berufsorientierungsmaßnahmen immer wichtiger. Denn der digitale Wandel führt dazu, dass traditionelle Vorstellungen von Arbeit zunehmend durch vernetzte Systeme, Algorithmen, Cloud-Lösungen und datenbasierte Entscheidungen ergänzt werden. Für Jugendliche bedeutet dies den Zugang zu modernen Lern- und Arbeitswelten, internationalen Karrierewegen und der Möglichkeit, Innovation aktiv mitzugestalten.

Die IT-Branche ist zudem besonders dynamisch: Programmiersprachen, Sicherheitsanforderungen, Tools und Technologien wie Künstliche Intelligenz entwickeln sich in kurzen Innovationszyklen weiter. Jugendliche benötigen daher eine Berufsorientierung, die nicht nur technische Grundlagen vermittelt, sondern auch Problemlösungskompetenz, Adaptionsfähigkeit und die Bereitschaft zum lebenslangen Lernen fördert.

Im Rahmen dieses Dokuments werden deshalb IT-Berufsorientierungsinhalte für Jugendliche zwischen 13 und 16 Jahren entwickelt. Dazu entstehen praxisnahe Materialien und methodisch moderne Workshop-Konzepte, die realistische Einblicke in verschiedene IT-Berufe – insbesondere den Bereich Cybersicherheit – geben. Die Inhalte bauen auf bisherigen Aktivitäten des Projekts auf, darunter ein Serious-Game-Tool, die Analyse des Wissensstands und Interesses Jugendlicher sowie die Untersuchung des Qualifikationsbedarfs von Betrieben im Grenzraum Österreich–Ungarn.

Lernziele

Die Jugendlichen …

- verstehen, was Cybersicherheit bedeutet und warum sie wichtig ist.
- kennen typische Aufgaben von Cybersecurity-Fachkräften.
- können grundlegende Sicherheitsrisiken erkennen (Passwörter, Phishing, Social Engineering).
- führen einfache, spielerische Sicherheitsanalysen durch.
- erkennen, welche Stärken und Interessen zu diesem Beruf passen.

DER BERUF – „CYBER SECURITY PROFESSIONAL“

Quelle: https://www.bic.at/berufsinformation.php?beruf=cyber-security-professional_m-w-d

Cyber Security bzw. Cybersicherheit bezeichnet den Schutz von Computersystemen und -netzwerken, Datenbanken, Serversystemen und anderen IT-Infrastrukturen vor dem Diebstahl oder der Beschädigung ihrer Hardware, Software oder elektronischer Daten sowie vor der Unterbrechung oder Fehlleitung. Ziel ist es, das Risiko von Cyber-Angriffen zu reduzieren und vor der unbefugten Ausnutzung von Systemen, Netzwerken und Daten zu schützen.

Cyber Security Professionals (m./w./d.) sind spezialisierte Informatiker:innen und IT-Spezialist:innen, die für die Sicherheit, insbesondere die Cybersicherheit von Servern, Computernetzwerken, Datenbanken etc. von Unternehmen und Organisationen verantwortlich sind. Zu ihren Kund:innen zählen beispielweise Banken und Versicherungen, öffentliche Organisationen und Unternehmen aller Branchen die datenintensive oder datensensitive IT-Systeme betreiben.

Fachkräfte in diesem Beruf sind für die Sicherheit der IT-Infrastruktur verantwortlich, implementieren und warten Sicherheitssoftware und -systeme und überwachen und aktualisieren deren Funktionalität (z. B. Firewalls, Antiviren-Programme, Spam-Filter). Sie identifizieren und beheben Schwachstellen, indem sie Phishing- und Hacking-Attacken simulieren. Sie beraten und informieren ihre Kund:innen über Internetkriminalität, Internetbetrug, Cyber-Attacken, und wie die betrieblichen Computer/IT-Systeme und IT-Infrastrukturen vor diesen geschützt werden können.

Cyber Security Professionals (m./w./d.) arbeiten im Team mit verschiedenen IT-Fachkräften wie z.B. Datenbankadministrator:innen, Netzwerkadministrator:innen, Webmaster (m./w./d.), Cloud-Architekt:innen und haben Kontakt zu Mitarbeiter:innen und Manager:innen der verschiedenen betrieblichen Abteilungen.

Beschäftigungsmöglichkeiten

- IT-Unternehmen und Unternehmensberatungen, Rechenzentren
- Banken- und Versicherungsgesellschaften
- Unternehmen aller Wirtschaftszweige
- Unternehmen und Organisationen, die personenbezogene Daten verarbeiten

- Verbände, Organisationen, Interessenvertretungen
- Werbung, Public Relations
- Ministerien, Behörden, Verwaltungseinrichtungen

Ausbildung & Qualifizierungswege (Österreich)

Der Beruf Cyber-Sicherheitsspezialist:in ist kein eigener Lehrberuf, sondern ein Spezialisierungs- und Tätigkeitsfeld innerhalb der IT. Der Einstieg erfolgt über fundierte IT-Grundausbildungen, die anschließend durch Praxis und gezielte Sicherheitsqualifikationen ergänzt werden.

Beruflicher Einstieg über Lehre

Ein praxisnaher Einstieg in cyberrelevante Tätigkeiten ist über folgende IT-Lehrberufe möglich:

- Applikationsentwicklung – Coding (Lehrberuf)
  → Schwerpunkt: Softwareentwicklung, logisches Denken, sichere Programmierung, Fehlersuche
- Informationstechnologie – Systemtechnik (Lehrberuf)
- Informationstechnologie – Betriebstechnik (Lehrberuf)

Diese Lehrberufe vermitteln zentrale Grundlagen für Cybersecurity, u. a.:

- Netzwerke und Server
- Betriebssysteme
- IT-Infrastruktur
- Grundlegende IT-Sicherheitsmaßnahmen
- Fehleranalyse und Systemüberwachung

Sie bilden eine solide Basis für spätere Tätigkeiten wie:

- IT-Systemadministrator:in mit Security-Fokus
- Junior Security Analyst
- SOC-Mitarbeiter:in (Security Operations Center)

Schulische Ausbildungswege

Alternativ oder ergänzend stehen schulische IT-Ausbildungen offen:

- Berufsbildende mittlere Schulen (BMS / IT-Fachschulen)

→ Grundlagen in IT, Netzwerken, Datensicherheit und Systembetreuung

- Höhere Technische Lehranstalten (HTL)

Fachrichtungen wie:

  - Informatik
  - Informationstechnologie

HTLs vermitteln vertiefte Kompetenzen in:

- Netzwerksicherheit
- Server- und Systemschutz
- Grundlagen der Cybersecurity
- sichere Software- und Systemarchitekturen

Die HTL ist einer der häufigsten Ausbildungswege in Richtung Cyber-Sicherheitsberufe.

Höhere Ausbildung (FH & Universität)

Für weiterführende oder spezialisierte Rollen im Bereich Cybersecurity:

- Fachhochschulen (FH)

z. B. Studiengänge in:

  - Informatik
  - IT-Security
  - System Engineering
  - Software Engineering

- Universitäten

z. B. Informatik oder verwandte technische Studienrichtungen, besonders relevant für:

  - Sicherheitsarchitektur
  - Penetration Testing
  - Forschung und Entwicklung

Zusatzqualifikationen & Zertifizierungen

Unabhängig vom Ausbildungsweg sind Spezialisierungen und Zertifikate entscheidend:

- IT-Security-Zertifikate (z. B. CompTIA Security+)
- Netzwerk-Zertifikate (z. B. Network+, CCNA)
- Linux- & Systemadministration
- Cloud- & Security-Zertifikate (AWS, Azure – Security-Fokus)

Diese Zertifikate weisen praxisnahe Sicherheitskompetenzen nach und sind für Arbeitgeber besonders relevant.

Cyber-Sicherheitsspezialist:in – mögliche Qualifizierungskette

→ Pflichtschule

→ IT-Lehre (Applikationsentwicklung oder Informationstechnologie – System-/Betriebstechnik) oder HTL

→ Berufspraxis in IT-Systemen / Netzwerken

→ Sicherheits-Spezialisierung & Zertifikate

→ Tätigkeit als Cyber-Sicherheitsspezialist:in

Berufliche Kompetenzen

Quelle: https://bis.ams.or.at/bis/beruf/593-Datensicherheitsexperte-expertin

- Betriebssystemkenntnisse (z.B. Windows, Linux)
- Datensicherheitskenntnisse (z.B. Wissen über Datensicherheitskonzepte)
- Elektronikkenntnisse (z.B. Wissen über Halbleitertechnologie)
- IT-Support – Kenntnisse (Durchführung von IT-Security-Workshops)
- Managementkenntnisse (z.B. Datenschutzmanagement)
- Netzwerktechnik-Kenntnisse (z.B. Netzwerkadministration)
- Programmiersprachen-Kenntnisse (z.B. Java)
- Rechtskenntnisse (z.B. Datenschutzgesetz)
- Datenbankkenntnisse

Was macht ein/e Cyber-Sicherheitsspezialist:in konkret?

- Systeme und Menschen schützen
    - Computer
    - Handys
    - Netzwerke
    - Firmen
    - Schulen
    - Krankenhäuser

- Sicherheitslücken finden (aber legal!)
    - Penetration Tester überprüfen Systeme, bevor echte Hacker sie finden.

- Angriffe erkennen und stoppen
    - Wenn in einer Firma etwas Verdächtiges passiert, finden Cyber-Teams heraus:
        1. Wer hat angegriffen?
        2. Was wurde gestohlen?
    - Wie verhindern wir es in Zukunft?

- Passwortrichtlinien, Datensicherheit & Schutzmaßnahmen erstellen

- Mitarbeitende schulen
    - Viele Angriffe passieren durch Menschen (z. B. Phishing). Cyber-Profis zeigen, wie man sicher arbeitet.

WORKSHOP-EINSTIEG – HACKER ODER BESCHÜTZER?

Einstieg

„Wir starten mit einer kleinen Vorstellung: Stellt euch vor… jemand findet euer Handy auf dem Schulhof. Es ist entsperrt. Die Person kennt euch nicht. Sie kann alles sehen.“
(Kurze Pause)

Auf dem Handy stehen eure Chats, Fotos, Standort, eure Apps sind offen, vielleicht sogar Passwörter gespeichert.

Viele denken: „Mein Handy ist ja nichts Besonderes.“

Aber: Auf unseren Geräten steckt heute fast unser ganzes Leben.

→ Realitätsbezug, der für Jugendliche nachvollziehbar ist

Frage an die Gruppe:

„Was wäre das Wichtigste zu schützen, wenn jemand euer Handy findet?“

Typische Antworten (falls niemand etwas sagt, kannst du diese einwerfen):

- Fotos
- Chats
- Passwörter
- Standort
- Social Media
- Spiele / Accounts
- Online-Banking (falls vorhanden)
- Kontaktliste
- Notizen

Weiterführende Impulsfragen, falls du sie brauchst:

- „Was könnte jemand mit eurem Instagram-Account machen?“
- „Warum wäre es schlimm, wenn jemand eure Chats liest?“
- „Wie schnell kann jemand eure Identität übernehmen?“

Im echten Leben gibt es Menschen, die genau dafür sorgen: dass niemand Unbefugtes an Daten, Geräte oder Informationen kommt. Diese Leute nennt man *Cybersecurity-Spezialist:innen*.

Sie schützen Computer, Firmen, Apps und Menschen — so wie ein Sicherheitsdienst, nur digital.

SICHERE PASSWÖRTER

Ziel

Die Schülerinnen und Schüler …

- verstehen, warum starke Passwörter wichtig sind.
- können schwache, mittlere und starke Passwörter unterscheiden.
- erstellen eigene Passwörter nach verschiedenen Schwierigkeitsgraden.
- lernen typische Strategien von Angreifern kennen (einfach erklärt).
- erkennen, wie Cybersecurity-Fachkräfte gefährliche Passwörter vermeiden

Auf diesen Websites kann die Stärke von Passwörtern gecheckt werden. Die zweite Seite zeigt auch an, wie oft das Passwort bereits im Internet aufgetaucht ist.

https://checkdeinpasswort.de/

https://nordpass.com/de/secure-password/

Einstieg

Der/die Vortragende zeigt typische schlechte Passwörter:

- 123456
- password
- hallo123
- Geburtsdatum
- Tiername + Zahl
- „qwertz“

Kurze Frage an die Gruppe: „Warum sind diese Passwörter schlecht?“

Mögliche Antworten, die du als Trainer:in aufgreifst:

- zu kurz
- leicht zu erraten

- oft verwendet
- persönliche Informationen
- stehen in Wörterlisten für Hacker

Hauptteil – Die Passwort-Challenge

Auftrag

Erstellt bitte drei Passwörter. Bitte keine echten Passwörter verwenden!
Erfindet sie einfach neu!

- Schlechtes Passwort
    - kurz, einfach, leicht zu erraten
    - z. B. „hase08“, „1234“, „schule12“
- Mittleres Passwort
    - kreativer, aber noch vorhersehbar
    - „Katze2024!“, „HalloLeute12“
- Starkes Passwort
    - mindestens 12 Zeichen
    - Mischung aus Groß-/Kleinbuchstaben, Zahlen, Sonderzeichen
    - am besten mit Merksatz

Beispiel:

- Merksatz: „Ich spiele jeden Freitag um 16 Uhr Fußball!“
- Passwort: IsjF@16UF!

Präsentation & Bewertung

Ablauf:

- Freiwillige lesen 1 Passwort vor (egal welches).

- Die Gruppe entscheidet mit einer einfachen Skala:

Schwach → leicht zu erraten

Mittel → besser, aber knackbar

Stark → sehr schwer zu knacken

Worauf soll die Gruppe achten?

- Länge
- Muster (1234, aaabbb)
- persönliche Daten
- Wörter aus dem Wörterbuch
- Sonderzeichen
- Groß-/Kleinschreibung
- Zufälligkeit

Fachinput – Wie knacken Hacker Passwörter?

Brute Force:

Der Computer probiert alle Möglichkeiten durch — Millionen pro Sekunde.

Wörterbuch-Angriff:

Hacker:innen nutzen Listen mit Millionen Passwörtern, die Menschen häufig verwenden.

Social Engineering:

Manchmal erraten Hacker:innen Passwörter, weil sie persönliche Infos kennen:

Geburtstag, Haustier, Lieblingsverein, ...

PHISHING

Ziele

Die Jugendlichen …

- erkennen typische Merkmale von Phishing-Nachrichten
- lernen 10–12 klare Warnsignale kennen
- können echte und gefälschte Nachrichten unterscheiden
- verstehen, wie Cybersecurity-Fachkräfte Angriffe analysieren
- wissen, wie sie sich selbst im Alltag schützen können

Frage an die Gruppe:

„Wer von euch hat schon einmal eine komische Nachricht bekommen — z. B. mit einem Link?“

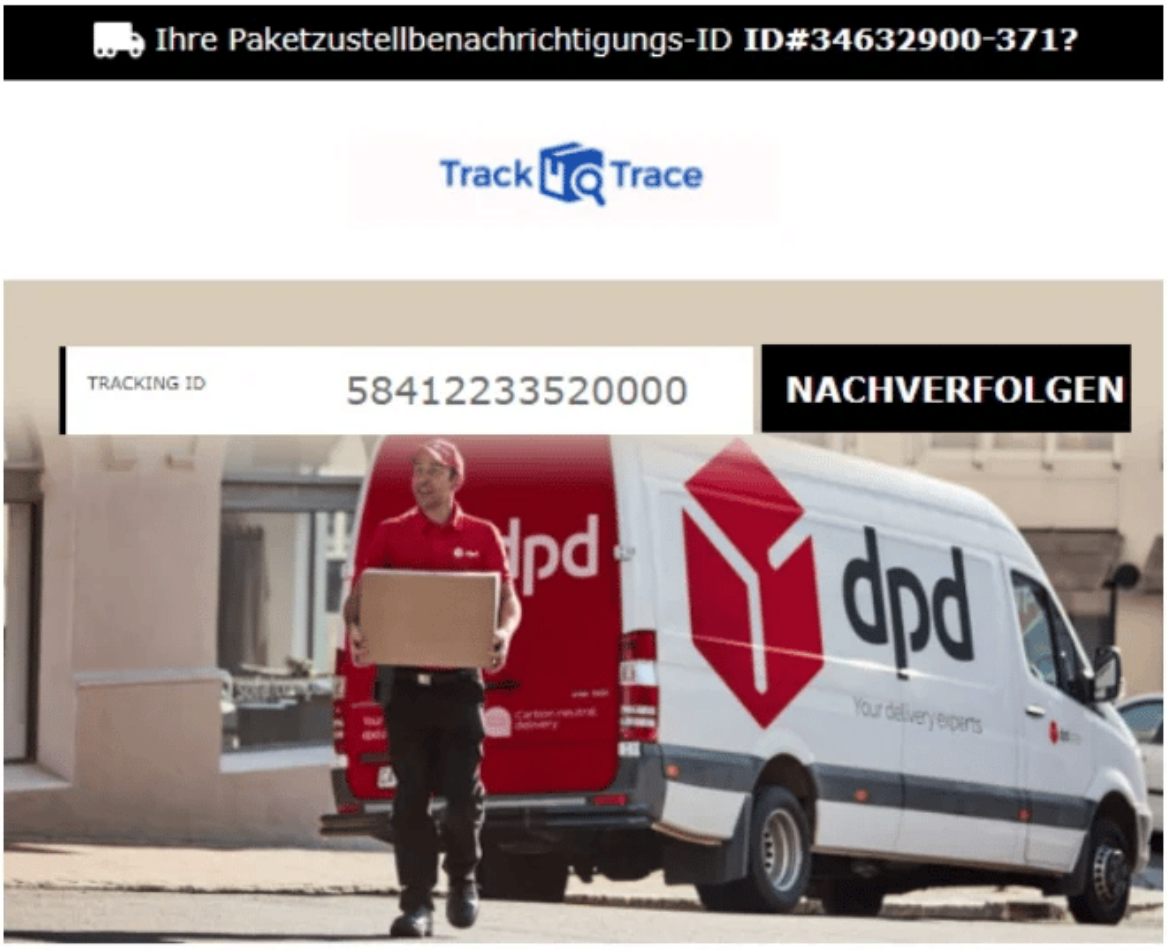
Dann erklären:

Phishing bedeutet: Man versucht euch zu täuschen, um eure Daten, Passwörter oder euer Geld zu stehlen. Das machen Cyberkriminelle weltweit — auch bei Jugendlichen.

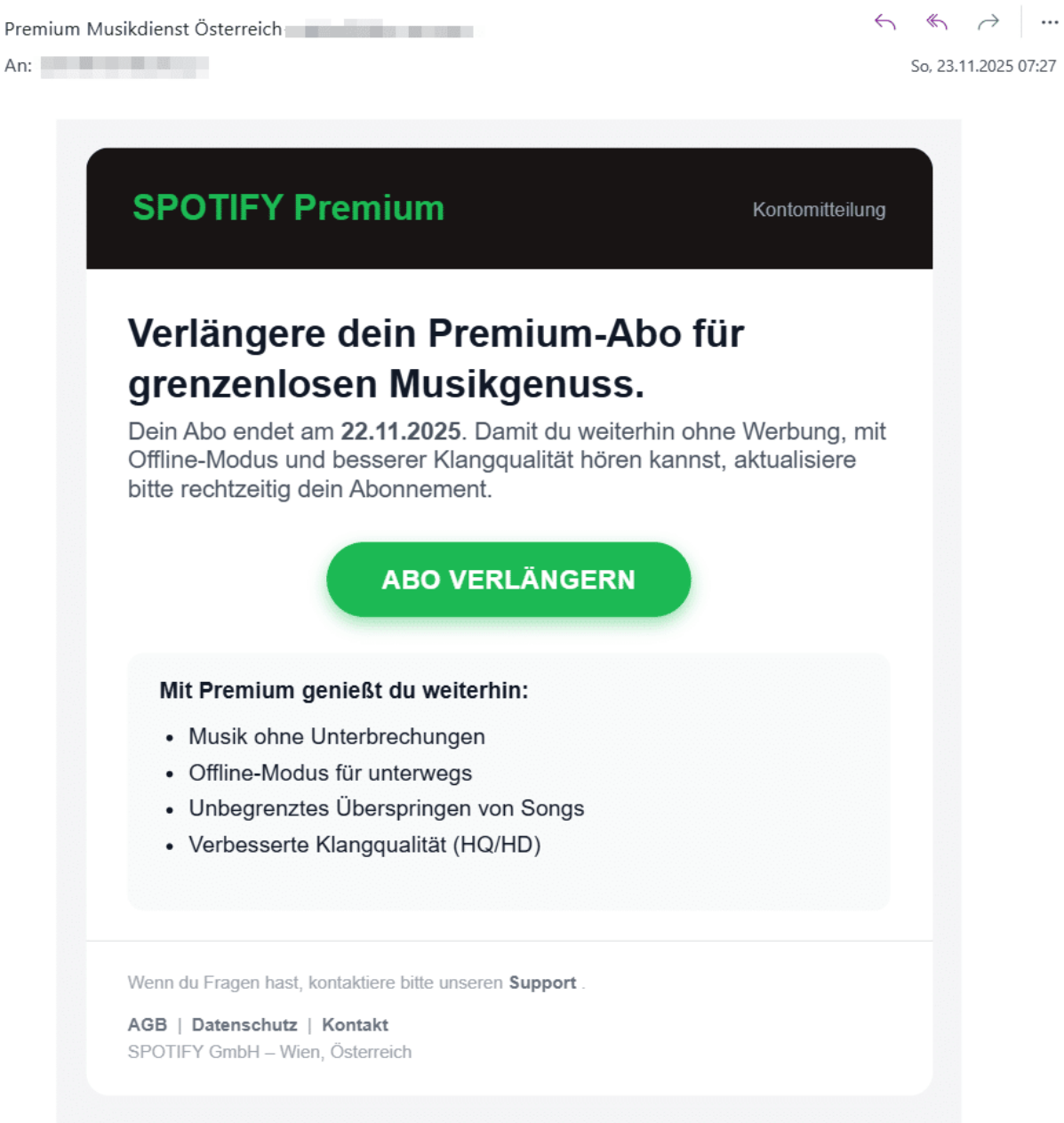
Das Wort kommt von Password+Fishing.

Beispiele

Beispiel 1 – Paketdienst



Beispiel 2 – Spotify



Beispiel 3 – Mail

> Ihr e-Mail ist gesperrt
>
> Microsoft konto team <privatemusteradresse@hotmail.de>
>
> Sehr geehrter-Nutzer
>
> Ihr zwei eingehenden e-Mails wurden auf ausstehender Status aufgrund der aktuellen Upgrade auf unsere Datenbank platziert. Um diese Mitteilungen zu erhalten, klicken Sie auf den untenstehenden Link, um Ihre Identität zu bestätigen und auf Antwort zu warten
>
> Klicken Sie hier um ihre Identität zu verifizieren
>
> Wir entschuldigen uns für die Unannehmlichkeiten und schätzen Ihr Verständnis.
>
> Mit freundlichen Grüßen
> Ihr Microsoft-Konto-Team

Beispiel 4 – Gewinnspiel

Beispiel 5 – Fake-Nachrichten

Beispiel 6 – A1 oder Drei SMS

Die 10 wichtigsten Warnsignale

- ungewöhnlicher Absender
- Druck erzeugen („Sofort klicken!“)
- Überraschungsgewinn
- Rechtschreibfehler
- Unbekannter Link
- Nachrichten von angeblichen Freunden mit neuer Nummer
- Fremde Login-Seiten
- Passwort sofort ändern müssen
- Anhänge von Unbekannten
- Emotionale Maschen (Angst, Stress, Neugier)

Abschluss-Reflexion

Fragen an die Gruppe:

„Welche dieser Warnsignale werdet ihr euch auf jeden Fall merken?“

„Was wäre euer Tipp an jemanden, der so eine Nachricht bekommt?“

„WIE HACKBAR IST EIN SCHUL-TAG?“

Bevor echte Cyberangriffe passieren, gibt es fast immer kleine Hinweise oder riskante Situationen. Cybersecurity-Spezialist:innen analysieren solche Situationen und bewerten, wie gefährlich sie sind.

Ziele

Die Jugendlichen …

- erkennen Sicherheitsrisiken im schulischen und privaten Alltag.
- lernen zu unterscheiden, welche Situationen harmlos oder gefährlich sind.
- entwickeln ein erstes Sicherheitsbewusstsein.
- verstehen, wie Cybersecurity-Profis reale Risiken analysieren.
- trainieren kritisches Denken und Teamkommunikation.

Gruppenarbeit - Auftrag

Die Jugendlichen arbeiten in Gruppen zu 2–4 Personen.

Jede Gruppe bekommt 6–8 Alltagssituationen aus der Schule oder Freizeit.

Sie sollen zu jeder Situation folgendes bewerten:

1. Wie gefährlich ist das? (Skala 1–5)
2. Warum?
3. Was wäre die sichere Lösung?

Situation A

Du findest einen USB-Stick am Schulhof.

→ Gefährlich (Malware, Datenklau)

Situation B

Ein Freund bittet dich um dein Hotspot-Passwort.

→ mittel/gefährlich (Mitnutzung, Haftung, Missbrauch)

Situation C

Jemand ruft deinen Namen und sagt: „Kannst du kurz dein Handy geben? Ich muss was googeln.“

→ gefährlich (Zugriff auf alles)

Situation D

Du bekommst eine Instagram-Nachricht: „Schau mal dieses Foto von dir 😳“ + Link

→ sehr gefährlich (Phishing, Accountübernahme)

Situation E

Ein Klassenkollege sagt sein Schul-WLAN-Passwort laut im Gang.

→ mittel (weitergegeben, Missbrauch)

Situation F

Die Passwortliste für den Computerraum liegt offen am Lehrer-PC.

→ sehr gefährlich (Zugriff auf alle Systeme)

Situation G

Du installierst eine App aus einem TikTok-Video, weil du „mehr Likes bekommst“.

→ gefährlich (Betrug, Malware)

Situation H

Eine E-Mail behauptet, es gäbe neue Hausaufgaben und man müsse dafür ein Passwort eingeben.

→ sehr gefährlich (Schul-Phishing)

Gruppenarbeit - Gruppenphase

Jede Gruppe stellt 1–2 Situationen kurz vor:

- ihre Einschätzung
- ihre Lösung

Der Trainer ergänzt jeweils:

- Was wäre die *professionelle Sicht* eines Cybersecurity-Spezialisten?
- Welche echten Risiken gibt es?
- Was ist die beste Vorgehensweise?

Du musst nicht alle Situationen präsentieren — wähle die spannendsten aus.

VR UND AR INHALTE

VR-Training: Fehleranalyse in einer IT-Infrastruktur

Im Bereich der Cybersicherheit können VR-Szenarien eingesetzt werden, um typische Aufgaben von IT-Sicherheitsfachkräften darzustellen.

In einer virtuellen Umgebung können Schülerinnen und Schüler beispielsweise:

- ungewöhnliche Systemmeldungen analysieren
- mögliche Sicherheitsprobleme identifizieren
- einfache Fehlerbehebungsmaßnahmen durchführen

Diese Simulationen verdeutlichen, dass Cybersicherheit nicht nur aus theoretischen Regeln besteht, sondern eng mit der Analyse technischer Systeme verbunden ist.

ANHANG: „WIE HACKBAR IST EIN SCHUL-TAG?“

Situation A *Du findest einen USB-Stick am Schulhof*	**Situation B** *Ein Freund bittet dich um dein Hotspot-Passwort*
Situation C *Jemand fragt: „Kannst du kurz dein Handy geben? Ich muss was googeln.“*	**Situation D** *Du bekommst eine Instagram-Nachricht: „Schau mal dieses Foto von dir 😳“ + Link*
Situation E *Ein Klassenkollege sagt sein Schul-WLAN-Passwort laut im Gang*	**Situation F** *Die Passwortliste für den Computerraum liegt offen am Lehrer-PC*
Situation G *Du installierst eine App aus einem TikTok-Video, weil du „mehr Likes bekommst“*	**Situation H** *Eine E-Mail behauptet, es gäbe neue Hausaufgaben und man müsse dafür ein Passwort eingeben*