SociALL

ZPŘÍSTUPNĚNÍ TECHNOLOGIÍ SOCIÁLNÍ PÉČE VŠEM

Téma 1.3. Základy online bezpečnosti a kybernetické ochrany

Financováno Evropskou unií. Názory vyjádřené jsou názory autora a neodráží nutně oficiální stanovisko Evropské unie či Evropské výkonné agentury pro vzdělávání a kulturu (EACEA). Evropská unie ani EACEA za vyjádřené názory nenese odpovědnost.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.

MedicalCar

åpenhet

Co-funded by the European Union

Obsah

Úvod do kurzu

1. Základy kybernetické a online bezpečnosti
2. Přehled nejčastějších hrozeb
3. Preventivní opatření
4. Osvědčené postupy a správné návyky
5. Užitečné nástroje a další zdroje

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

SociALL

Úvod do kurzu

1. O kurzu
2. Cílová skupina
3. Cíle školení

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

Úvod do kurzu

1. O kurzu

O čem je kurz?

Kurz "Základy online bezpečnosti a kybernetické ochrany" má pracovníkům v sociálních službách poskytnout základní znalosti a dovednosti pro **ochranu citlivých údajů a zajištění online bezpečnosti v** rámci jejich práce. Účastníci se dozvědí, jak **identifikovat** a **zmírnit** běžná rizika kybernetické bezpečnosti a jak přijmout **osvědčené postupy** a snadno proveditelná opatření pro online bezpečnost.

Proč na tom záleží?

Význam tohoto kurikula vyplynul z nadnárodního výzkumu projektu SociALL: kybernetická bezpečnost je obzvláště **významným a aktuálním** tématem v kontextu zvýšeného rizika kybernetické bezpečnosti, obav o zdraví a soukromí a integritu osobních údajů. Množící se kybernetické útoky na **zranitelné** organizace poskytující péči, jak ukázaly nedávné vlny vyděračských útoků na evropské nemocnice, vyžadují zvýšenou pozornost a znalosti.

Co-funded by the European Union

Úvod do kurzu

2. Cílová skupina

Pro koho je kurz určen?

Tento kurz může absolvovat prakticky **každý pracující v oblasti péče,** protože každý z nich denně používá digitální nástroje a je tak vystaven kybernetickým rizikům. Kurz se skládá převážně z vysvětlení , tipů a osvědčených postupů, které lze u většiny z nich aplikovat individuálně a bez důležitých technických dovedností. Většina tohoto obsahu může pracovníkům posloužit v jejich profesním životě, ale uplatní se i při osobním používání digitálních nástrojů.

Mohu se jím řídit?

Tento učební plán je přizpůsoben **všem pracovníkům** a poskytuje spíše základní, užitečné úvody a pokyny ke kybernetické a online bezpečnosti. Každý člověk, který je zvyklý používat digitální nástroj ve svém profesním životě, je proto schopen tento kurz absolvovat, pochopit a poučit se z něj.

Co-funded by the European Union

Úvod do kurzu

3. Cíle školení

SociALL

Co se mohu z kurzu naučit?

- Pochopit **význam** kybernetické a online bezpečnosti.
- Porozumět **rizikům** a nejčastějším **hrozbám**
- Pochopit **lidský faktor** při kybernetických útocích
- Uplatňovat **snadno proveditelná opatření na** ochranu dat a bezpečnost online
- Využit užitečných **zdrojů**, **nástrojů** a celosvětově uznávaných **osvědčených postupů ke** zvýšení bezpečnosti.

Co se tím změní?

Na konci školení budou účastníci a jejich organizace schopni lépe:

- **Začlenit** online bezpečnost do svých aktivit
- **Identifikovat** a **řešit rizika** kybernetické bezpečnosti
- Změnit **procesy,** které je činí **zranitelnými,** na bezpečnější procesy.
- **Školit a radit** svým kolegům v této oblasti, aby se vytvořila **bezpečnější organizační kultura.**
- **Předávat** tyto znalosti **zranitelným pacientům,** pokud pracovníci sociální péče vnímají **rizika.**

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

SociALL

1. Základy kybernetické a online bezpečnosti

1. Význam kybernetické bezpečnosti a bezpečnosti online
2. Pochopení odpovědnosti pečovatelů za integritu údajů o pacientech
3. Lidské chyby a nedbalost jsou hlavní vstupní branou pro kybernetickou kriminalitu.
4. Co můžeme dělat? Identifikovat a ošetřit zranitelná místa člověka

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
MPWA
Medicalscan
åpenhet
Co-funded by the European Union

1. Základy kybernetické a online bezpečnosti

1.1. Význam kybernetické bezpečnosti a bezpečnosti online

Kybernetická bezpečnost není jen módní slovo

Je to štít, který nás chrání před různými online riziky, jako jsou krádeže identity, finanční podvody, krádeže osobních údajů, kybernetické útoky, které vyřadí z provozu celou organizaci atd.

Kybernetická bezpečnost je trojí ochrana

V sektoru péče má kybernetická bezpečnost za úkol chránit jednotlivé sociální pracovníky, jejich organizace a pacienty.

Kybernetické útoky jsou novou kriminalitou

Jak ukázala nedávná vlna útoků vyděračského softwaru na pečovatelská zařízení (nemocnice, domovy důchodců atd.), jsou kybernetické útoky v pečovatelském sektoru stále nebezpečnější a hrozivější.

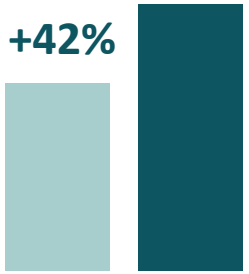
Závěr: **Nebezpečí** kybernetické kriminality nebylo nikdy tak velké jako dnes. Naše **závislost na** digitálních nástrojích ve všech aspektech života z nás činí **zranitelný** cíl, pokud nepodnikneme žádné **kroky k** zajištění naší digitální bezpečnosti.

Co-funded by the European Union

1. Základy kybernetické a online bezpečnosti

1.1. Význam kybernetické bezpečnosti a bezpečnosti online

Několik čísel ze zprávy "Trendy kybernetických útoků: Zpráva za polovinu roku 2022" ukazuje, že nebezpečí je reálné. Jen v roce 2022:



Kybernetické útoky na zdravotnická zařízení vzrostly o **42 % ve srovnání s** předchozím obdobím.

Průměrné celkové náklady na únik dat ve zdravotnictví činily **10,10 milionu amerických dolarů na** jeden incident.

Zdravotnické organizace zaznamenaly **1 426** (zdokumentovaných) **útoků týdně po** celém světě.

Ve třetím čtvrtletí roku 2022 se **1 ze 42** zdravotnických organizací stala obětí útoku ransomwaru.

Závěr: **Nebezpečí** kybernetické kriminality nebylo nikdy tak velké jako dnes. Naše **závislost na** digitálních nástrojích ve všech aspektech života z nás činí **zranitelný** cíl, pokud nepodnikneme žádné **kroky k** zajištění naší digitální bezpečnosti.

Co-funded by the European Union

1. Základy kybernetické a online bezpečnosti

1.2. Pochopení odpovědnosti pečovatelů za integritu údajů o pacientech

SociALL

Důvěra je základním kamenem a základem vztahu mezi ošetřovatelem a pacientem. Ústřední součástí této důvěry je schopnost odpovědně zacházet s citlivými a osobními údaji pacientů a chránit je.

Údaje o pacientech představují pokladnici **osobních** a často **citlivých** informací.

- Lékařská anamnéza
- Plán léčby
- Hygiena života
- Kontaktní údaje
- Číslo sociálního pojištění

Pracovníkům v oblasti péče je svěřeno velké množství **osobních** a **zdravotních** údajů, které mohou zajímat **různé subjekty,** od společností prodávajících produkty až po podvodníky, kteří hledají snadné oběti, nebo osoby se špatnými úmysly všeho druhu.

A co je ještě důležitější a bez ohledu na jejich hodnotu, tyto údaje jsou **osobní** a **soukromé**. Pracovníci v oblasti péče nesou velkou odpovědnost za jejich zachování, kteří jim svěřují své údaje.

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

1. Základy kybernetické a online bezpečnosti

1.2. Pochopení odpovědnosti pečovatelů za integritu údajů o pacientech

Digitální zpracování údajů o pacientech sice usnadnilo život pracovníkům v oblasti péče a zvýšilo jejich efektivitu, představuje však **zranitelnost** a **novou oblast, kterou je třeba chránit**.

Co GDPR ? HIPAA?

Existují **právní povinnosti, které** zajišťují minimální ochranu a iniciují pohyb. Pečovatelé by však neměli přijímat opatření na ochranu údajů pouze proto, aby tyto povinnosti respektovali: jejich **etickou povinností je** zachovávat **důstojnost** a **soukromí** pacientů.

Ochrana údajů přesahuje rámec dodržování zákonných povinností.

Pracovníci v oblasti péče si musí uvědomit, jaký **dopad** může mít **narušení bezpečnosti údajů**, a pochopit **váhu a důležitost** své **odpovědnosti**. Na tomto uvědomění závisí důvěra jejich pacientů a také morální závazek pracovníků v oblasti péče – chránit své pacienty.

Co-funded by the European Union

1. Základy kybernetické a online bezpečnosti

SociALL

1.3. Lidské chyby a nedbalost jsou hlavní vstupní branou pro kybernetickou kriminalitu.

Kyberzločinci využívají **lidské chyby a nedbalost.** Představují nejjednodušší **vstupní bránu** a rovnají se tomu, když po nočním odchodu z pečovatelského zařízení necháte dveře dokořán bez dozoru.

Hackování softwaru a databází zneužitím jejich **technických zranitelností** existuje, ale je velmi vzácné a tvoří jen malou část kybernetických útoků. V naprosté většině případů kyberzločinci jednoduše procházejí **dveřmi, které nechali otevřené** lidé - ať už chybou, nebo nedbalostí, aby získali **neoprávněný přístup** a **ohrozili citlivé informace**.

"Jsem pečovatelka. Proč by mě to mělo zajímat?"

Téměř u všech kybernetických útoků, které byly v poslední době zaznamenány v odvětví sociální péče (phishing, ransomware atd.), nebyl hlavní příčinou narušení vadný antivirový program, slabý software nebo neoptimální technická architektura: tyto útoky téměř neustále využívají **lidské chyby,** často ze strany samotného personálu.

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

1. Základy kybernetické a online bezpečnosti

1.4. Co můžeme dělat? Identifikovat a ošetřit zranitelná místa člověka

Kybernetická bezpečnost v sektoru péče není jen o úsilí jednotlivců - chyba jednoho z nich má dopad na všechny ostatní. Jde o **kolektivní odpovědnost**, **informovanost**, zavádění **osvědčených postupů** a **školení**.

Kybernetická bezpečnost je institucionálně komplexní záležitost, protože chyba jednoho má dopad na všechny (příkladem je ransomware, jehož obětí se stala řada nemocnic). Vzhledem k této všezahrnující povaze je kybernetická bezpečnost o **zlepšení kolektivní obrany** proti kybernetickým hrozbám, a ne pouze o zlepšení chování jednotlivců.

Jako taková znamená **kolektivní úsilí** o **zvýšení povědomí, zvýšení odpovědnosti, vzdělávání zaměstnanců v** oblasti kybernetických hrozeb, kolektivní přijetí a uplatňování procesů, které integrují **osvědčené postupy** atd.

Na **úrovni jednotlivce** kybernetická bezpečnost neznamená pouze **dodržování protokolů** a procesů, ale také pochopení vlastní pozice jako **aktéra kybernetické bezpečnosti instituce,** což znamená **kritické myšlení a zvyšování povědomí o** rizicích, podíl na **školení nebo mentoring, aktivní zapojení** a odpovědnost.

Co-funded by the European Union

1. Základy kybernetické a online bezpečnosti

1.4. Co můžeme dělat? Identifikovat a ošetřit zranitelná místa člověka

Kybernetická bezpečnost je nejistá věda: k narušení dochází i v dobře chráněných a vzdělaných strukturách. Organizace by neměly zanedbávat **nápravná opatření a připravenost v** případě narušení.

I při zlepšeném přístupu ke kybernetické bezpečnosti, lepších procesech, vzdělanějším personálu atd. může stále docházet k narušení bezpečnosti dat a kybernetickým útokům, i když v podstatně menší míře. Stoprocentní ochrana neexistuje, a proto je pro pečovatelské instituce zásadní, aby měly k dispozici kompletní strategie, které lze v případě narušení bezodkladně zavést, a aby byly připraveny na krizové řízení, protiopatření, obnovení kontroly a snížení dopadů.

Nicméně tyto strategie je třeba vypracovat spíše na úrovni **technických týmů.** Nápravná opatření a připravenost jako takové nejsou součástí tohoto učebního plánu, ačkoli jsou pro každou organizaci poskytující péči naprosto nezbytné.

Co-funded by the European Union

SociALL

2. Přehled nejčastějších hrozeb

1. Ochrana pacientů/klientů
2. Phishingové útoky
3. Malware
4. Sociální inženýrství

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
MPSA
Medicalscan
åpenhet
Co-funded by the European Union

2. Přehled nejčastějších hrozeb

2.1. Ochrana pacientů/klientů

Online hrozby se mohou zaměřit a poškodit

Jednotlivé zaměstnance

Organizace poskytující péči

Pacienty/ Klienty

Zejména určité kategorie pacientů/klientů, které jsou více **ohroženy** kybernetickými útoky – jako jsou **izolovaní starší lidé**.

Pracovníci v oblasti péče mohou chránit své klienty, pokud zjistí online riziko pro jejich bezpečnost, a to tak, že

Pozorují jejich chování online

Diskutují s nimi a ptají se jich na jejich online život.

Identifikují potenciální rizika v jejich chování na internetu

Varujípřed zjištěnými nebezpečími

Vzdělávají je v online bezpečnosti

Co-funded by the European Union

2. Přehled nejčastějších hrozeb

2.2. Phishingové útoky

Phishingové útoky jsou **podvodné** pokusy o **získání citlivých informací** vydáváním se za **důvěryhodné** subjekty. V oblasti péče mohou mít phishingové útoky většinou podobu:

Podvody s kompromitací firemních e-mailů ("velrybaření")

Sofistikované útoky, jejichž cílem je přimět zaměstnance k převodu finančních prostředků nebo k vyzrazení citlivých informací.

Tyto podvody se často odehrávají prostřednictvím **e-mailu na** finančních nebo účetních odděleních, kde **se vydávají za** vysoce postavené vedoucí pracovníky nebo oprávněné osoby.

Tyto podvodné e-maily obvykle požadují **urgentní** platby, změny údajů o dodavateli nebo citlivé informace o zaměstnancích a využívají **hierarchického vztahu** mezi odesílatelem a příjemcem.

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

Zdroj: Proofpoint

CLUES

- ✓ Odesílatel využívá vyšší hierarchickou pozici
- ✓ Pocit naléhavosti - není čas na kontrolu / protesty
- ✓ Odesílatel nemůže telefonovat, pouze psát.
- ✓ Podvržený název domény e-mailu odesílatele

Co-funded by the European Union

2. Přehled nejčastějších hrozeb

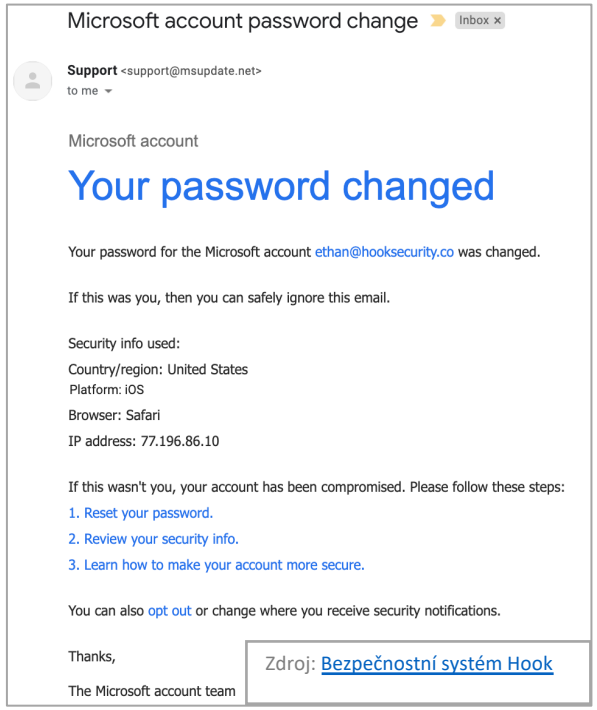
2.2. Phishingové útoky

Phishingové útoky jsou **podvodné** pokusy o **získání citlivých informací** vydáváním se za **důvěryhodné** subjekty. V oblasti péče mohou mít phishingové útoky většinou podobu:

Phishingové útoky s cílem získat pověření

Phishingové útoky zaměřené na získávání pověření se zaměřují na **krádež** uživatelských jmen, hesel a dalších přihlašovacích **údajů za** účelem získání **neoprávněného přístupu** do systémů péče. Tyto podvody často používají přesvědčivé **repliky** legitimních přihlašovacích stránek, například portálů EMR nebo intranetů.

Útočníci posílají phishingové e-maily nebo přesměrovávají oběti na **škodlivé webové stránky,** kde zadávají své přihlašovací údaje a **nevědomky** tak poskytují kyberzločincům klíče k citlivým údajům organizace.



Microsoft account password change Inbox ×

Support <support@msupdate.net>
to me

Microsoft account

Your password changed

Your password for the Microsoft account ethan@hooksecurity.co was changed.

If this was you, then you can safely ignore this email.

Security info used:
Country/region: United States
Platform: iOS
Browser: Safari
IP address: 77.196.86.10

If this wasn't you, your account has been compromised. Please follow these steps:
1. Reset your password.
2. Review your security info.
3. Learn how to make your account more secure.

You can also opt out or change where you receive security notifications.

Thanks,
The Microsoft account team

Zdroj: Bezpečnostní systém Hook

CLUES

- ✓ Podvržený název domény e-mailu odesílatele (např.: @msupdate.net)
- ✓ Odlišný design e-mailu od běžných e-mailů společnosti
- ✓ Žádost o reakci na něco, co jste neudělali (např.: doručení balíčku, který jste si neobjednali).

Co-funded by the European Union

2. Přehled nejčastějších hrozeb

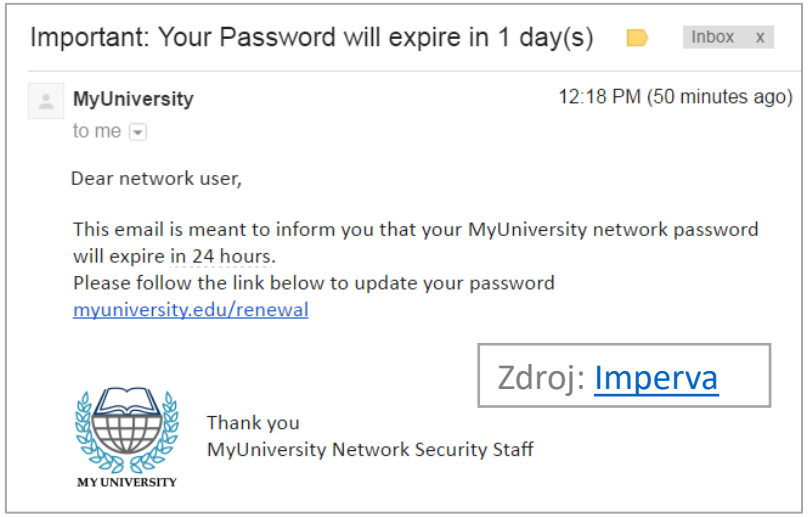
2.2. Phishingové útoky

Phishingové útoky jsou **podvodné** pokusy o **získání citlivých informací** vydáváním se za **důvěryhodné** subjekty. V oblasti péče mohou mít phishingové útoky většinou podobu:

Phishingové e-maily s malwarem

Cílem phishingových e-mailů se škodlivým softwarem je přimět příjemce ke stažení a spuštění **škodlivého softwaru**. Tyto e-maily často obsahují **infikované přílohy** nebo **odkazy na** napadené webové stránky.

Zdravotnické organizace jsou **obzvláště zranitelné** vůči útokům malwaru, protože úspěšné narušení může ohrozit záznamy pacientů, narušit provoz nebo dokonce ohrozit životy.


Important: Your Password will expire in 1 day(s) Inbox x

MyUniversity 12:18 PM (50 minutes ago)
to me

Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

Zdroj: Imperva

MY UNIVERSITY

Thank you
MyUniversity Network Security Staff

CLUES

- ✓ Pravopisné, gramatické a interpunkční chyby
- ✓ Odkazy v těle e-mailu, které přesměrovávají na neočekávané stránky (po najetí na odkaz se zobrazí adresa URL).
- ✓ Hrozba (např. zablokovaný účet) nebo pocit naléhavosti.
- ✓ Přílohy, které jste si nevyžádali / nespustili.
- ✓ Neobvyklá žádost, tón nebo pozdrav

Co-funded by the European Union

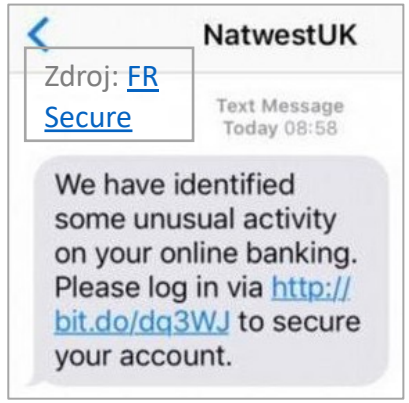
2. Přehled nejčastějších hrozeb

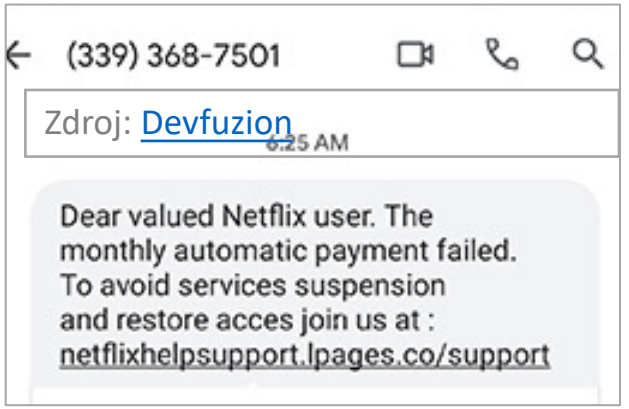
2.2. Phishingové útoky

Phishingové útoky jsou **podvodné** pokusy o **získání citlivých informací** vydáváním se za **důvěryhodné** subjekty. V oblasti péče mohou mít phishingové útoky většinou podobu:

Vishingové a smishingové útoky

Vishing (prostřednictvím hlasových zpráv nebo telefonních hovorů) a **smishing** (prostřednictvím SMS) může být některý z předchozích phishingových útoků. Jednoduše nahrazují tradiční e-mail jiným komunikačním prostředkem (SMS, hovor apod.).





CLUES

Vishing

- ✓ Náročný tón: podvodníci využívají strachu nebo paniky
- ✓ Žádost o důvěrné nebo osobní informace
- ✓ Předstíraný volající: většina organizací, které podvodníci předstírají, že zastupují, by nevolala.

Smishing

- ✓ Neznámé číslo, není uvedeno na internetu
- ✓ Navštivte webové stránky předstíraného odesílatele - např. banky na svých webových stránkách píší, že neposílají SMS.
- ✓ Kontaktujte přímo zákaznický servis společnosti

Co-funded by the European Union

2. Přehled nejčastějších hrozeb

2.2. Phishingové útoky

Phishingové útoky jsou **podvodné** pokusy o **získání citlivých informací** vydáváním se za **důvěryhodné** subjekty.

Několik čísel z roku **2022** ukazuje, jak rozšířený, sofistikovaný a nebezpečný je phishing (Zdroj: Stationx.net)

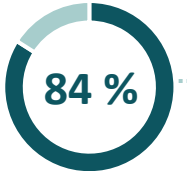
3.4 B

Phishing je **nejčastější formou počítačové kriminality**. Odhadem **3,4 miliardy e-mailů denně jsou** phishingové útoky zasílané kyberzločinci. Jedná se o více než **bilion** phishingových e-mailů / **rok**.

36 % všech případů narušení bezpečnosti dat zahrnuje phishing.

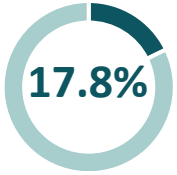
Vydávání se za e-mailové zprávy představuje odhadem **1,2 % veškerého e-mailového provozu na celém** světě.

1.2 %



84 % organizací se v roce 2022 stalo terčem alespoň **jednoho pokusu o phishing.**

Průměrná míra kliknutí u phishingové kampaně je **17,8 %.**



3 %

V průměru 3 % zaměstnanců kliknou na škodlivý odkaz ve phishingovém e-mailu.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.

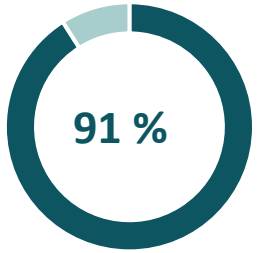
Co-funded by the European Union

2. Přehled nejčastějších hrozeb

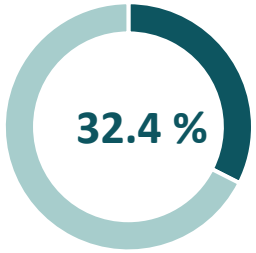
2.2. Phishingové útoky

Phishingové útoky jsou **podvodné** pokusy o **získání citlivých informací** vydáváním se za **důvěryhodné** subjekty.

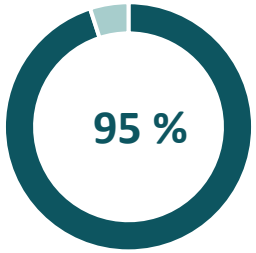
Několik čísel z roku **2022** ukazuje, jak rozšířený, sofistikovaný a nebezpečný je phishing (Zdroj: Stationx.net)



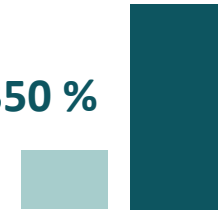
všech kybernetických útoků začíná podvodným **e-mailem.**



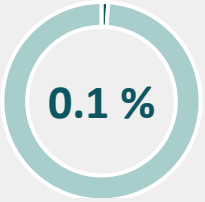
nevyškolených zaměstnanců může naletět phishingovým podvodům.



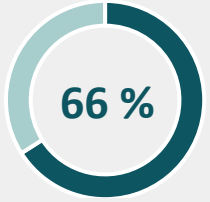
úspěšných narušení je přímo způsobeno **lidskou chybou.**



Malé organizace se stávají o **350 %** častěji **terčem phishingu** než větší organizace.



0,1 % všech e-mailových phishingových útoků je zodpovědných za **66 %** všech narušení. (*obvykle cílené, personalizované "spear-phishingové" útoky).*



Co-funded by the European Union

2. Přehled nejčastějších hrozeb

2.3. Malware

Malware je souhrnný pojem zahrnující různé typy škodlivého softwaru určeného k narušení, poškození nebo získání přístupu do počítačových systémů, sítí nebo zařízení. V oblasti péče mají malwarové programy většinou podobu:

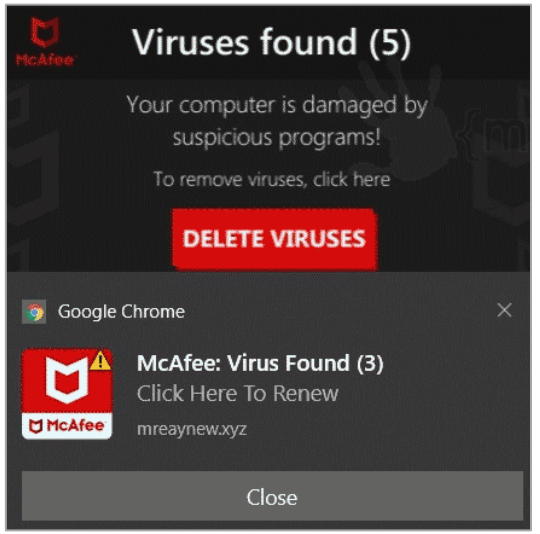
Viry

Viry jsou škodlivé programy, které **infikují** jiné soubory nebo software v počítači a po **spuštění** infikovaných souborů se replikují. Mohou způsobit poškození dat, softwaru a hardwarových komponent.

Například phishingové e-maily nebo SMS s malwarem mohou uživatele přimět ke kliknutí na infikované **odkazy** nebo stažení **souborů.** Tyto infikované soubory nebo odkazy se "aktivují" až po kliknutí uživatele, proto je třeba být při přijímání nevyžádaných e-mailů opatrný.

POZOR

Mnoho podvodníků využívá váš **strach z virů k** tomu, aby vás infikovali: pokud vyskakovací zpráva antivirového programu, který nemáte, upozorňuje na možnou infekci vašeho zařízení a nabízí její řešení kliknutím na tlačítko nebo zavoláním na číslo, nereagujte, může vás to velmi dobře přivést ke spuštění viru.



Zdroj: Komunita společnosti Microsoft

Co-funded by the European Union

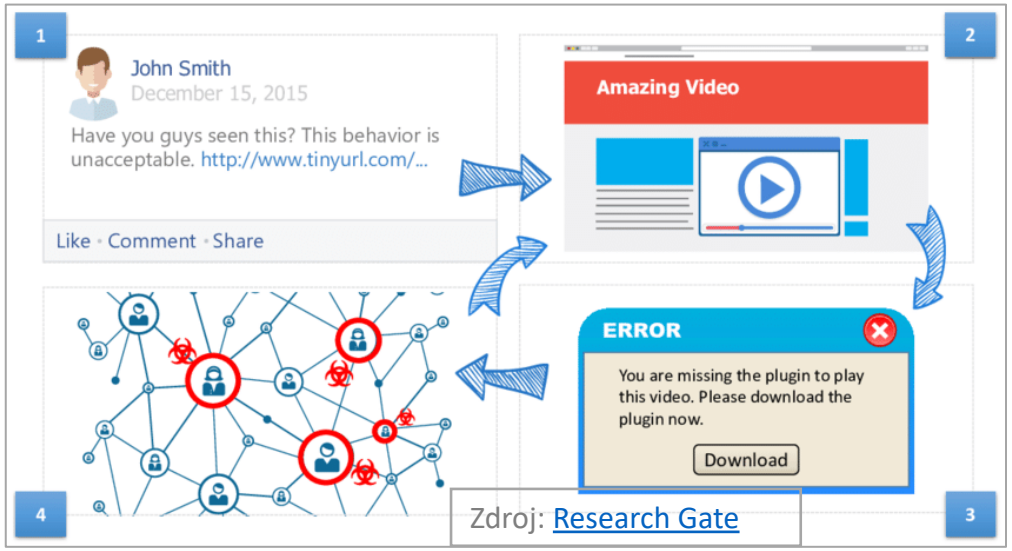
2. Přehled nejčastějších hrozeb

2.3. Malware

Malware je souhrnný pojem zahrnující různé typy škodlivého softwaru určeného k narušení, poškození nebo získání přístupu do počítačových systémů, sítí nebo zařízení. V oblasti péče mají malwarové programy většinou podobu:

Trojské koně

Trojské koně jsou škodlivý software **maskovaný jako legitimní software**. Uživatele oklamou a přimějí je k instalaci, často tak, že se tváří jako neškodné soubory nebo aplikace. Po instalaci mohou trojské koně provádět různé škodlivé činnosti, například krást citlivá data, měnit informace nebo poskytovat útočníkům neoprávněný přístup. Trojské koně jsou často spouštěny podvodnými e-maily nebo zprávami.



Zdroj: Research Gate

CLUES

- ✓ Počítač pracuje pomaleji než obvykle.
- ✓ V zařízení se objevují neautorizované aplikace.
- ✓ Časté pády a zamrzání zařízení.
- ✓ Častá vyskakovací okna.
- ✓ Některé aplikace se nespustí.
- ✓ Časté přerušování připojení k internetu.

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

2. Přehled nejčastějších hrozeb

2.3. Malware

Malware je souhrnný pojem zahrnující různé typy škodlivého softwaru určeného k narušení, poškození nebo získání přístupu do počítačových systémů, sítí nebo zařízení. V oblasti péče mají malwarové programy většinou podobu:

Ransomwares

Ransomware je typ malwaru, který zašifruje soubory v počítači nebo zařízení oběti a **znepřístupní** je, **dokud není zaplaceno výkupné**. Útoky ransomwaru obvykle požadují platbu v kryptoměně a mohou způsobit značné finanční ztráty a ztráty dat.

Cílem jsou zejména **nemocnice a zdravotnická zařízení,** jejichž systémy jsou pro jejich provoz životně důležité. V roce 2022 bylo **66 %** nemocnic v USA **cílem** (ne vždy obětí) útoku ransomwaru. Organizace ve zdravotnictví **zaplatily v** roce 2022 výkupné v přibližně **61 %** případů ransomwaru.

Zdroj: Healthcare IT News

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

2. Přehled nejčastějších hrozeb

2.3. Malware

Malware je souhrnný pojem zahrnující různé typy škodlivého softwaru určeného k narušení, poškození nebo získání přístupu do počítačových systémů, sítí nebo zařízení. V oblasti péče mají malwarové programy většinou podobu:

Červi

Červi jsou samostatné škodlivé programy, které se **replikují v** sítích a obvykle využívají zranitelnosti v operačních systémech nebo síťových protokolech.

Mohou se rychle šířit a způsobovat **přetížení sítě** nebo provádět jiné škodlivé činnosti.

Spywares

Spywarové programy jsou určeny k **tajnému sledování** a shromažďování informací o činnostech uživatele v počítači nebo zařízení.

Mohou **sledovat stisky kláves, pořizovat snímky obrazovky, zaznamenávat zvyky při procházení** a krást **citlivé informace,** jako jsou hesla a finanční údaje.

Addwares

Addwares jsou nechtěný software, který zobrazuje **reklamy,** často ve formě vyskakovacích oken nebo přesměrování prohlížeče.

Ačkoli adware není ve své podstatě škodlivý, může **snižovat výkon systému**, ohrožovat **soukromí** uživatele a vést k **dalším infekcím,** pokud není odstraněn.

Co-funded by the European Union

2. Přehled nejčastějších hrozeb

2.3. Malware

Malware je souhrnný pojem zahrnující různé typy škodlivého softwaru určeného k narušení, poškození nebo získání přístupu do počítačových systémů, sítí nebo zařízení. V oblasti péče mají malwarové programy většinou podobu:

Keyloggery

Keyloggery jsou typem špionážního softwaru, který zaznamenává **stisky kláves** zadané uživatelem a zachycuje citlivé informace, jako jsou **hesla**, **uživatelská jména** a údaje o **kreditních kartách.**

Útočníci mohou pomocí keyloggerů ukrást osobní údaje a spáchat krádež identity.

Botnety

Botnety jsou **sítě napadených počítačů** nebo zařízení ovládaných útočníky.

Botnety mohou být použity k provádění distribuovaných útoků typu **DDoS (**Distributed **Denial-of-Service)**, rozesílání **nevyžádaných e-mailů** nebo k provádění jiných škodlivých činností **bez vědomí jejich vlastníků**.

“Zadní vrátka” - backdoors

Zadní vrátka jsou **skryté vstupní body** nebo zranitelnosti, které útočníci záměrně vytvořili v softwaru nebo systémech a které umožňují **neoprávněný přístup za účelem budoucího zneužití nebo ovládnutí**.

Tato zadní vrátka umožňují útočníkům **tajně a na dálku** převzít kontrolu nad zařízením, instalovat další škodlivý software, zaznamenávat stisky kláves atd.

Co-funded by the European Union

2. Přehled nejčastějších hrozeb

2.3. Malware

Tyto různé typy malwaru jsou často kombinovány v rámci jednoho programu nebo souboru. Několik čísel z roku **2022** ukazuje, jak jsou malwary rozšířené, sofistikované a nebezpečné (Zdroj: Getastra.com)

Denně je odhaleno **560 000 nových kusů** malwaru. V současné době existuje více než **1 miliarda malwarových** programů.

Každou minutu se obětí ransomwarových útoků stanou **4 společnosti.** Nejčastějším cílem je **sektor péče, který** také platí nejvíce výkupného. Průměrné náklady na ransomwarový útok činí **4,54 milionu dolarů.**

Při incidentech s ransomwarem se pouze **50 %** organizací, které zaplatily **výkupné,** podařilo **získat zpět svá data**. **64 %** organizací, které se staly terčem ransomwarových útoků, bylo skutečně **infikováno**.

Za posledních deset let došlo k **87% nárůstu** počtu malwarových infekcí. **Trojské koně** tvoří **58 %** veškerého počítačového malwaru. Předpokládá se, že náklady na počítačovou kriminalitu dosáhnou v **roce 2023 výše 8 bilionů dolarů**.

Co-funded by the European Union

2. Přehled nejčastějších hrozeb

2.4. Sociální inženýrství

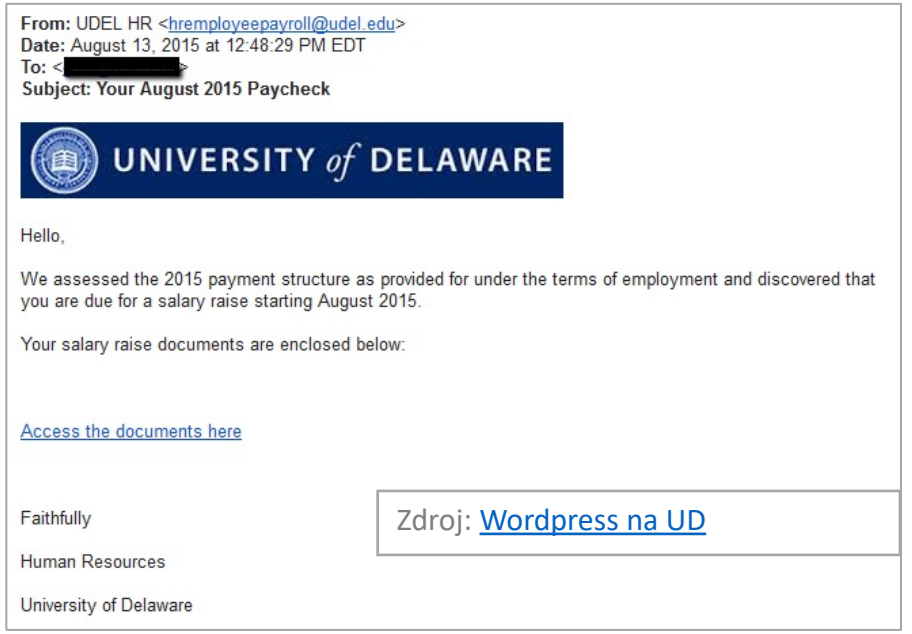
Sociálním inženýrstvím se rozumí využívání sociálních taktik ke zneužití důvěry, nedbalosti nebo nevědomosti zaměstnanců za účelem získání důvěrných informací. Zatímco phishingové a malwarové útoky často využívají těchto zranitelností a **překrývají se** se sociálním inženýrstvím, čisté sociální inženýrství využívá **sociální taktiky** příměji a může zahrnovat:

Spear phishing

Spear phishing je **cílená forma phishingu,** která **útok přizpůsobuje** konkrétním osobám nebo organizacím.

Útočníci shromažďují informace o svých cílech ze sociálních médií, veřejných databází nebo z předchozích interakcí, aby přizpůsobili phishingové e-maily a zvýšili pravděpodobnost úspěchu.

Spear phishingové zprávy mohou obsahovat škodlivý software různých typů, přímo požadovat osobní údaje (např. telefonní číslo pro vyřešení "naléhavé záležitosti"), žádat o úhradu faktury apod.



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

Zdroj: Wordpress na UD

2. Přehled nejčastějších hrozeb

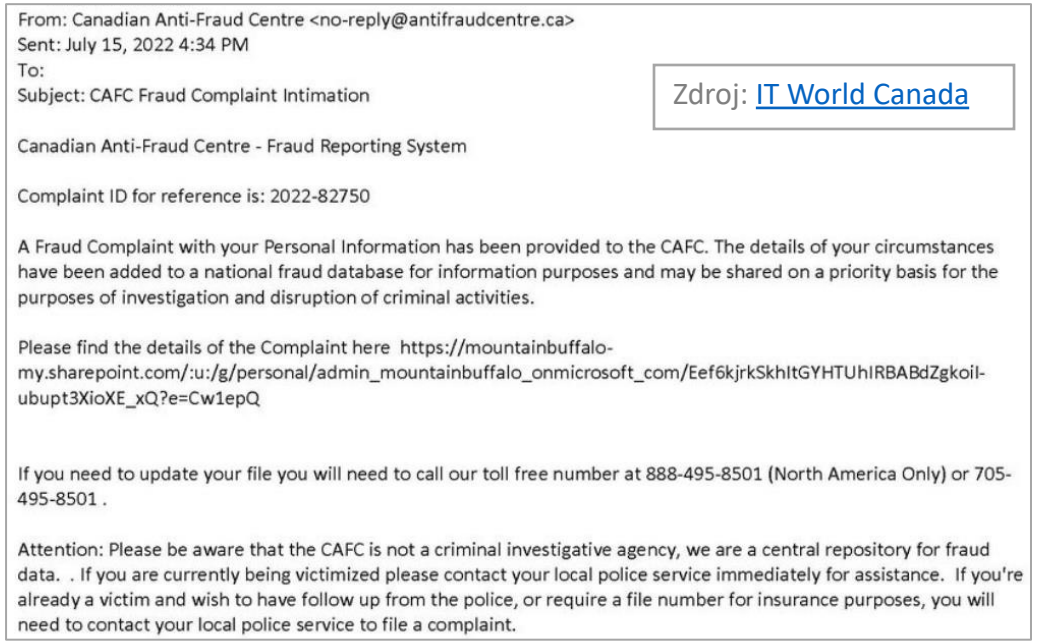
2.4. Sociální inženýrství

Sociálním inženýrstvím se rozumí využívání sociálních taktik ke zneužití důvěry, nedbalosti nebo nevědomosti zaměstnanců za účelem získání důvěrných informací. Zatímco phishingové a malwarové útoky často využívají těchto zranitelností a **překrývají se** se sociálním inženýrstvím, čisté sociální inženýrství využívá **sociální taktiky** příměji a může zahrnovat:

Pretexting

Záminka spočívá ve vytvoření **vymyšleného scénáře nebo záminky, která** má jednotlivce přimět k prozrazení důvěrných informací nebo k provedení určitých činností.

Útočníci se často vydávají za **důvěryhodné subjekty, jako jsou** pracovníci IT podpory, pracovníci orgánů činných v trestním řízení nebo vedoucí pracovníci společnosti, aby získali důvěru cíle a získali citlivé informace. Podvody s předstíráním mohou mít velmi podobné výsledky jako jakýkoli typ phishingového podvodu, tedy požadavek na platbu, krádež pověření nebo osobních údajů atd.



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

Zdroj: IT World Canada

Canadian Anti-Fraud Centre - Fraud Reporting System

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/Eef6kjrkSkhItGYHTUhIRBABdZgkoil-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.

Co-funded by the European Union

2. Přehled nejčastějších hrozeb

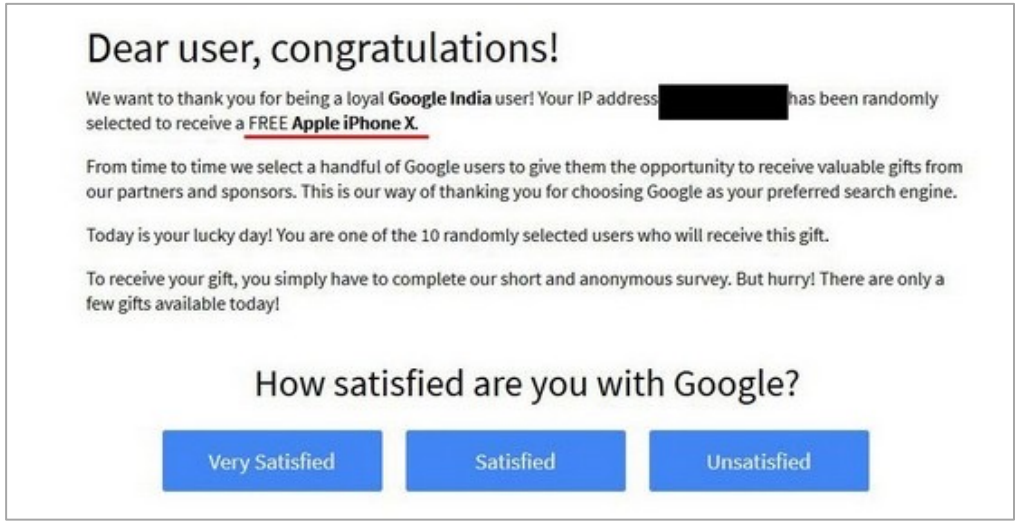
2.4. Sociální inženýrství

Sociálním inženýrstvím se rozumí využívání sociálních taktik ke zneužití důvěry, nedbalosti nebo nevědomosti zaměstnanců za účelem získání důvěrných informací. Zatímco phishingové a malwarové útoky často využívají těchto zranitelností a **překrývají se** se sociálním inženýrstvím, čisté sociální inženýrství využívá **sociální taktiky** příměji a může zahrnovat:

Vábení

Návnada se spoléhá na **zvědavost nebo chamtivost** lidí a láká je ke stažení škodlivých souborů nebo návštěvě napadených webových stránek. Útočníci nabízejí **lákavé návnady,** jako je například bezplatné stažení softwaru, filmů nebo dárkových karet, které obsahují malware nebo vedou na phishingové stránky.

Vábení je často spojeno s určitým druhem záminky, spear phishingem, vydáváním se za někoho jiného atd., aby se zaměřilo na **zranitelnost** uživatele a zvýšilo **důvěryhodnost** odesílatele.



Zdroj: Dummies.com

Co-funded by the European Union

2. Přehled nejčastějších hrozeb

2.4. Sociální inženýrství

Sociálním inženýrstvím se rozumí využívání sociálních taktik ke zneužití důvěry, nedbalosti nebo nevědomosti zaměstnanců za účelem získání důvěrných informací. Zatímco phishingové a malwarové útoky často využívají těchto zranitelností a **překrývají se** se sociálním inženýrstvím, čisté sociální inženýrství využívá **sociální taktiky** příměji a může zahrnovat:

Přeprava na zádech (Piggybacking):

"Tailgating" neboli "piggybacking" znamená **fyzické získání neoprávněného přístupu** do vyhrazených oblastí nebo systémů sledováním oprávněné osoby.

Útočníci využívají **lidské zdvořilosti nebo nedostatečné informovanosti** ke vstupu do zabezpečených prostor bez řádného oprávnění.

Útoky na vodní díry

Útoky typu Watering hole se zaměřují na konkrétní skupiny nebo organizace a **infikují webové stránky, které jejich členové navštěvují,** malwarem.

Útočníci kompromitují legitimní webové stránky a **šíří malware** nic netušícím návštěvníkům, přičemž využívají jejich důvěry v napadené stránky.

Vydávání se za někoho jiného (krádež identity):

Většina taktik phishingu zahrnuje určitou formu vydávání se za někoho jiného. Některé však obsahují další prvky, které zvyšují důvěryhodnost a představují **krádež identity**.

Může jít o ukradená nebo padělaná pověření a dokumenty, prvky vytvořené IA apod., které **klamou** o jejich pravosti.

Co-funded by the European Union

2. Přehled nejčastějších hrozeb

2.4. Sociální inženýrství

Sociální inženýrství často představuje bránu pro doručení malwaru nebo přimění oběti k provedení určité akce. Několik čísel z roku **2023** ukazuje, jak rozšířené, sofistikované a nebezpečné je sociální inženýrství (Zdroj: Resmo).

90 %

90 % případů narušení bezpečnosti dat a **98 %** kybernetických útoků (úspěšných i neúspěšných) mělo prvky sociálního inženýrství.

$4.5 M

Průměrné **náklady na** narušení dat iniciované technikami sociálního inženýrství **přesahují 4,5 milionu dolarů**.

700

Typická organizace (v USA) byla **ročně** terčem více než **700 útoků sociálního inženýrství.**

+ 354 %

Útoky na převzetí účtu se v roce 2023 meziročně zvýšily o 354 %.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.

Medicalscar

åpenhet

Co-funded by the European Union

SociALL

3. Preventivní opatření

1. Zabezpečení heslem
2. Dvoufaktorové ověřování (2FA)
3. Anti-virus
4. Aktualizace softwaru
5. Zabezpečení sítě
6. Zálohování dat

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

3. Preventivní opatření

3.1. Zabezpečení heslem

Proč je to důležité?

Zabezpečení heslem je **první slabinou, kterou** kyberzločinci využívají. **Silnější** hesla (tj. složitější a rozmanitější) je obtížnější uhodnout nebo odhalit pomocí útoků hrubou silou, a proto mohou být přijatelnou a užitečnou **první linií obrany** proti kybernetickým útokům.

Co mohu dělat?

- Nastavte si **silná** hesla: alespoň **16** znaků, velká a malá písmena, číslice a speciální znaky.
- **Přeměňte věty** na hesla namísto slov pomocí kódu pro přeměnu různých typů písmen. Například: "Icàre@b0utSecur1ty!"
- Používejte **správce hesel, kteří** si hesla pamatují za vás a generují je.

Co může moje organizace udělat?

- Nakonfigurujte své systémy (e-mail, nástroje pro online zasílání zpráv, ERP, CRM atd.) tak, aby uživatelé museli **pravidelně obnovovat svá hesla.** Tím se zkrátí doba platnosti daného hesla.
- Nakonfigurujte **pravidla pro zadávání hesel,** abyste zajistili, že uživatelé nepoužijí **stejné heslo dvakrát** a že heslo je **dostatečně silné**.
- Vynucení všeobecné **obnovy hesla** po narušení.

Co-funded by the European Union

3. Preventivní opatření

3.1. Zabezpečení heslem

Proč je to důležité?

Zabezpečení heslem je **první slabinou, kterou** kyberzločinci využívají. **Silnější** hesla (tj. složitější a rozmanitější) je obtížnější uhodnout nebo odhalit pomocí útoků hrubou silou, a proto mohou být přijatelnou a užitečnou **první linií obrany** proti kybernetickým útokům.

ZOOM na správce hesel

- Správci hesel **ukládají hesla a zbavují vás povinnosti** si je pamatovat. Jako cloudová řešení zůstávají **přístupné** i **z jiných zařízení**.
- Registraci hesla lze provést **ručně** nebo **automaticky.** Správce hesel můžete také nastavit tak, aby při připojování k účtům automaticky vyplňoval pole s heslem.
- Správci hesel mohou pro každý z vašich účtů **vygenerovat jedinečná a velmi silná hesla** a zapamatovat si je za vás. Ani je nebudete muset znát.
- Stačí si zapamatovat **jedno velmi silné heslo** - to, které vám umožní přístup ke správci hesel.

Užitečné nástroje

- Dashlane
- 1Heslo
- LastPass
- Bitwarden

Co-funded by the European Union

3. Preventivní opatření

3.2. Dvoufaktorové ověřování (2FA)

SociALL

Proč je to důležité?

2FA výrazně zvyšuje bezpečnost: tato metoda ověřování vyžaduje pro přihlášení k účtu použití nejméně **dvou zařízení,** přičemž obě musí být předem **zaregistrována** a **důvěryhodná.** Tato metoda nejenže dává uživateli **kontrolu** nad účtem, který mohl být kompromitován, ale může také **indikovat, že** byl kompromitován.

Co mohu dělat?

- **Povolte 2FA** co nejdříve - po prozrazení hesla nebo účtu už bude pozdě.
- Ve většině softwaru a webových stránek ji můžete povolit v části **Nastavení > Zabezpečení (**IOS a Microsoft, služby Google, sociální sítě atd.).
- Nejpoužívanější a nejspolehlivější metodou je použití **dvou zařízení** patřících uživateli (např. telefonu a počítače) registrovaných na účtu.

Co může moje organizace udělat?

- U většiny systémů může oddělení IT vynutit **2FA pro** všechny uživatele v **celém systému.** 2FA může být také označováno jako "dvoufázové ověření" nebo "vícefaktorové ověřování".
- To však vyžaduje, aby všichni **zaměstnanci měli přístup ke 2 zařízením, v** ideálním případě pouze pro pracovní použití, což nemusí být tento případ. Případně lze zaměstnance **vyzvat, aby** si zapnuli 2FA.

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

3. Preventivní opatření

3.2. Dvoufaktorové ověřování (2FA)

Proč je to důležité?

2FA výrazně zvyšuje bezpečnost: tato metoda ověřování vyžaduje pro přihlášení k účtu použití nejméně **dvou zařízení,** přičemž obě musí být předem **zaregistrována** a **důvěryhodná.** Tato metoda nejenže dává uživateli **kontrolu** nad účtem, který mohl být kompromitován, ale může také **indikovat, že** byl kompromitován.

Jak to mám udělat?

- Pracovní prostor Google (Gmail, Gdrive, Kalendář atd.)
- Microsoft 365 (Outlook, OneDrive, Teams atd.)
- Slack
- Zoom

A další - obecně dostupné v **bezpečnostní relaci Nastavení** pro většinu digitálních nástrojů - včetně těch pro osobní použití (sociální sítě, bankovnictví, elektronické obchodování, vládní aplikace a webové stránky atd.).

Co-funded by the European Union

3. Preventivní opatření

3.3. Anti-virus

Proč je to důležité?

Antivirové programy chrání svého majitele tím, že **skenují potenciální hrozby a odhalují rizika,** od pokusů o podvodný e-mail nebo malware až po podvodné webové stránky a programy. Tato ochrana se vztahuje i mimo počítač, a to na všechna **externí zařízení, která** s ním komunikují, například USB klíče, které mohou být také nositeli škodlivého softwaru.

Co mohu dělat?

- **samostatně nainstalujte** antivirový software, pokud jej neposkytuje vaše organizace (nebo **se zasaďte o to, aby byl nainstalován** v rámci celé organizace). Nechráněné počítače jsou **snadným cílem** kyberzločinců.
- Nezapomeňte, že antivirové programy jsou dalšími vrstvami **zabezpečení, které stále závisí na lidském** faktoru: zachovávejte **stejnou úroveň ostražitosti** online, ať už jste "chráněni", nebo ne.

Co může moje organizace udělat?

Oddělení IT může a **mělo by** instalovat, konfigurovat a spravovat aktualizace **antivirového softwaru pro celý systém, aby byla zajištěna** lepší ochrana digitálního zabezpečení organizace.

Užitečné nástroje

ESET
Kaspersky
Bitdefender
AVG

Co-funded by the European Union

3. Preventivní opatření

3.4. Aktualizace softwaru

SociALL

Proč je to důležité?

Aktualizace softwaru a operačních systémů brání kyberzločincům ve zneužití známých **bezpečnostních problémů**: dodavatelé softwaru pravidelně provádějí zátěžové testy svého zabezpečení. Když zjistí potenciální bezpečnostní chyby, **vydávají aktualizace, které** tyto chyby odstraňují nebo je činí nezneužitelnými.

Co mohu dělat?

Neodkládejte aktualizaci veškerého softwaru a aplikací, které používáte (osobně i pracovně), když obdržíte oznámení o aktualizaci. Pravidelně ověřujte, zda je vše aktuální v centru aplikací.

Co může moje organizace udělat?

Oddělení IT může konfigurovat automatické aktualizace operačních systémů a aplikací používaných v celé organizaci a vybrat, kdy a jak často je instalovat, aniž by došlo k narušení provozu.

Jak to mám udělat?

V systému Windows

Na Macu

V systému Android

V systému IOS

Užitečné nástroje

Správa aktualizací v systému Windows

Zapnutí automatických aktualizací aplikací

Aktualizace systému MacOS v počítači Mac

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.

MedicalCar

åpenhet

Co-funded by the European Union

3. Preventivní opatření

3.5. Zabezpečení sítě - VPN

Proč je to důležité?

Pokud je nutné, aby pracovníci přistupovali k informacím **zvenčí, je pro** pracovníky IT obtížnější mít pod **kontrolou všechny bezpečnostní aspekty**. **Virtuální privátní sítě (VPN)** umožňují vytvořit **přímou, bezpečnou a izolovanou síť** mezi dvěma počítači a umožňují jim vzájemnou interakci a výměnu dat.

Jak to funguje?

VPN je technologie, která vytváří **bezpečné a šifrované** připojení přes internet. VPN šifruje data přenášená mezi zařízením uživatele a serverem VPN, čímž brání třetím stranám v zachycení a přístupu k datům. Toto šifrování představuje **další úroveň zabezpečení a** zajišťuje, že citlivé informace, jako jsou hesla, údaje o kreditních kartách a osobní komunikace, zůstanou v bezpečí.

V kontextu pracovníků v oblasti péče VPN většinou **zabezpečují vzdálený přístup k** soukromým sítím a zdrojům, jako jsou podnikové intranety, servery nebo databáze, zejména pro pracovníky v terénu. Budou také zajišťovat **vyšší bezpečnost** pro ty, kteří se připojují k internetu prostřednictvím **veřejných** a zpravidla nezabezpečených **sítí Wifi**.

Co-funded by the European Union

3. Preventivní opatření

3.5. Zabezpečení sítě - VPN

Proč je to důležité?

Pokud je nutné, aby pracovníci přistupovali k informacím **zvenčí, je pro** pracovníky IT obtížnější mít pod **kontrolou všechny bezpečnostní aspekty**. **Virtuální privátní sítě (VPN)** umožňují vytvořit **přímou, bezpečnou a izolovanou síť** mezi dvěma počítači a umožňují jim vzájemnou interakci a výměnu dat.

Co může moje organizace udělat?

VPN by mělo v případě potřeby instalovat **technické oddělení organizace,** protože se většinou používá jako **celosystémové geografické rozšíření stávající sítě,** což brání jednotlivým uživatelům v samostatné instalaci. Jednotlivci však mohou VPN **obhajovat** před svým IT oddělením nebo vedením.

Sítě VPN mohou vyžadovat **instalaci softwaru** do počítačů, které mají být propojeny, a také **metodu ověřování** před přístupem do sítě. Mohou být nakonfigurovány tak, aby fungovaly pouze na určitých zařízeních, na určitých místech a v určitou dobu, a omezovaly tak přístup zvenčí, přičemž pracovníkům, kteří to potřebují, stále umožňují přístup k potřebným datům.

Co-funded by the European Union

3. Preventivní opatření

3.6. Zálohování dat

SociALL

Proč je to důležité?

Jednou z hlavních hrozeb kybernetických útoků je **pozměňování citlivých údajů,** konkrétně údajů o pacientech. Zajištění jejich bezpečnosti a integrity je naprosto zásadní, a to i tváří v tvář kybernetické hrozbě. Klíčem k zajištění integrity dat je robustní **strategie institucionálního zálohování dat s postupy** pravidelného **zálohování** a **vysokou mírou dodržování předpisů ze strany personálu.**

Co mohu dělat?

- Prvním opatřením pro zajištění integrity a bezpečnosti dat je pro jednotlivé pracovníky **dodržování různých protokolů** stanovených technickým oddělením, absolvování **pravidelných školení** a **seriózní** a důsledné **posuzování této záležitosti.**
- Jako aktér zabezpečení vlastní organizace **se** můžete také **zajímat o** strategii zálohování dat, **navrhovat** a **prosazovat její** změny.

Co může moje organizace udělat?

Za návrh a realizaci **strategie institucionálního zálohování dat je** zodpovědné technické oddělení. Taková strategie by měla zahrnovat **opatření zajišťující dodržování předpisů ze strany zaměstnanců,** postupy pro **pravidelné zálohování dat** na **cloudová úložiště** (Gdrive, Onedrive atd.) nebo síťová úložiště, která poskytují bezpečnostní síť pro **rychlou obnovu dat v** případě porušení integrity dat.

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

4. Osvědčené postupy a správné návyky

1. Fyzický prostor
2. Zabezpečené procházení
3. Zabezpečené odesílání e-mailů
4. Bezpečné používání sociálních médií
5. Zabezpečení mobilních zařízení
6. Zabezpečení heslem

Co-funded by the European Union

4. Osvědčené postupy a správné návyky

4.1. Fyzický prostor

Kybernetická bezpečnost začíná offline: před nastavením technické ochrany se ujistěte, že jste svůj fyzický prostor uspořádali bezpečným způsobem, který sníží nebezpečí a zranitelnost.

1. Uzamčení nepoužívaných zařízení
2. Zabezpečte svůj pracovní prostor před neoprávněným přístupem
3. Přijměte zásady čistého stolu
4. Použití zástěn pro ochranu soukromí
5. Skartace citlivých dokumentů
6. Nezapisujte si hesla
7. Dávejte pozor na surfování na ramenou
8. Povolení šifrování celého disku

Co-funded by the European Union

4. Osvědčené postupy a správné návyky

4.1. Fyzický prostor

Kybernetická bezpečnost začíná offline: před nastavením technické ochrany se ujistěte, že jste svůj fyzický prostor uspořádali bezpečným způsobem, který sníží nebezpečí a zranitelnost.

1. Když zařízení nepoužíváte, zamkněte je

Počítač, notebook, tablet nebo telefon vždy **zamykejte,** když je nepoužíváte, zejména ve veřejných nebo sdílených prostorách. Používejte silná hesla, kódy PIN nebo biometrické ověřování (např. otisky prstů nebo rozpoznávání obličeje), abyste zabezpečili svá zařízení a zabránili neoprávněnému přístupu.

Tipy

- V systému Windows zamkněte obrazovku pomocí klávesové zkratky Windows + L.
- V počítači Mac zamkněte obrazovku pomocí klávesové zkratky Control-Command-Q.

2. Zabezpečte svůj pracovní prostor před neoprávněným přístupem

- Udržujte svůj pracovní prostor **bez přístupu nepovolaných osob**. Zajistěte, aby fyzické přístupové body, jako jsou dveře, okna nebo vchody, byly zabezpečeny a monitorovány, aby se zabránilo neoprávněnému vstupu do vašeho pracovního prostoru nebo prostor.
- **Uzamykejte** zásuvky, skříně nebo kartotéky s citlivými dokumenty, zařízeními nebo paměťovými médii, pokud se nepoužívají.
- Zabezpečte **periferní zařízení,** jako jsou klávesnice, myši a externí paměťová zařízení (USB, pevný disk atd.), a uložte je do uzamčených zásuvek nebo skříní.

Co-funded by the European Union

4. Osvědčené postupy a správné návyky

4.1. Fyzický prostor

Kybernetická bezpečnost začíná offline: před nastavením technické ochrany se ujistěte, že jste svůj fyzický prostor uspořádali bezpečným způsobem, který sníží nebezpečí a zranitelnost.

3. Přijměte politiku čistého stolu

Dodržujte **zásadu čistého stolu a** odstraňte ze svého stolu citlivé dokumenty, poznámky nebo hesla, když nejste přítomni. Fyzické dokumenty ukládejte bezpečně, nejlépe do uzamčených skříní nebo zásuvek.

Tipy

Osvědčeným postupem je snaha o "stůl s nulovým počtem papírů", na kterém jsou pouze aktuálně používané papíry. Je prokázáno, že to nejen zvyšuje efektivitu a snižuje stres, ale také snižuje riziko ponechání důležitých informací na viditelném místě nepovolanými osobami.

4. Používejte zástěny pro ochranu soukromí

Používejte **obrazovky nebo filtry soukromí** na počítači nebo mobilních zařízeních, abyste zabránili neoprávněnému sledování obrazovky. Obrazovky pro ochranu soukromí nutí diváky stát přesně před zařízením a zabraňují surfování přes rameno. V některých zařízeních jsou zabudovány nebo je lze stáhnout.

Tipy

- V počítačích s integrovanou obrazovkou soukromí ji aktivujete stisknutím klávesy F12 nebo Fn + D.
- V systému Android jsou nejlépe hodnocené aplikace pro ochranu soukromí 1) Privacy Screen, 2) Screen Guard privacy, 3) Privacy filter.

Co-funded by the European Union

4. Osvědčené postupy a správné návyky

4.1. Fyzický prostor

Kybernetická bezpečnost začíná offline: před nastavením technické ochrany se ujistěte, že jste svůj fyzický prostor uspořádali bezpečným způsobem, který sníží nebezpečí a zranitelnost.

5. Skartace citlivých dokumentů

Skartovat nebo bezpečně zlikvidovat fyzické dokumenty obsahující citlivé informace, jako jsou finanční záznamy, osobní doklady apod., než je zlikvidujete. Nevyhazujte je jednoduše do koše, aniž byste dokument **alespoň roztrhli.**

Tipy

Přestože recyklace je dnes povinností každého pracovníka, nezapomeňte, že volný papír je často ponechán bez dozoru před recyklací, a pokud je citlivý, může vaši organizaci vystavit potenciálnímu narušení bezpečnosti.

6. Nezapisujte si hesla

Nezapisujte si hesla ani kódy PIN na lepicí papírky, do zápisníků **ani do** fyzických dokumentů. Pokud je zapsání hesla nezbytně nutné, udělejte to na místě, kde ho nelze najít, a zašifrujte ho kódem, který dokážete rozluštit pouze vy (např.: č. dětí sestry / měsíc narozenin psa atd.).

Tipy

Místo toho používejte renomovaného správce hesel, který hesla bezpečně ukládá a spravuje. Jediné heslo, které si budete muset pamatovat, je heslo správce hesel.

Co-funded by the European Union

4. Osvědčené postupy a správné návyky

4.1. Fyzický prostor

Kybernetická bezpečnost začíná offline: před nastavením technické ochrany se ujistěte, že jste svůj fyzický prostor uspořádali bezpečným způsobem, který sníží nebezpečí a zranitelnost.

7. Dávejte pozor na surfování na ramenou

Dávejte pozor na své okolí a chraňte svou obrazovku a klávesnici před pohledem nepovolaných osob, zejména na veřejných místech. Při zadávání kódu PIN nebo hesla na bankomatech, klávesnicích nebo mobilních zařízeních **si klávesnici chraňte.**

Tipy

- Ochrana soukromí je dobrý způsob, jak se bránit surfování přes rameno.
- Na veřejných místech si raději sedejte zády ke zdi, abyste zabránili surfování po ramenou zezadu.

8. Povolení šifrování celého disku

Povolte v zařízeních **šifrování celého disku,** abyste ochránili data uložená na pevném disku nebo úložném médiu zařízení. Tím zajistíte, že i v případě krádeže nebo ztráty zařízení nebudou mít neoprávnění uživatelé přístup k datům bez šifrovacího klíče.

Tipy

- V systému Windows povolte šifrování v nabídce Nastavení > Soukromí a zabezpečení.
- Většina mobilních operačních systémů dnes disponuje také funkcemi umožňujícími vzdálené odstranění dat v případě ztráty zařízení.

Co-funded by the European Union

4. Osvědčené postupy a správné návyky

4.2. Zabezpečené procházení

Při **procházení internetu dbejte** na dodržování následujících osvědčených postupů.

1. Používejte zabezpečené webové stránky (HTTPS)
2. Aktualizujte svůj software a operační systém
3. Používání blokátorů reklam a filtrů obsahu
4. Buďte opatrní při stahování
5. Anonymní prohlížení
6. Pravidelně čistěte mezipaměť prohlížeče a soubory cookie

Co-funded by the European Union

4. Osvědčené postupy a správné návyky

4.2. Zabezpečené procházení

Při **procházení internetu dbejte** na dodržování následujících osvědčených postupů.

1. Používejte zabezpečené webové stránky (HTTPS)

V adrese URL webové stránky hledejte **HTTPS,** abyste zajistili bezpečné připojení při přenosu citlivých informací, jako jsou přihlašovací údaje nebo finanční údaje. Vyhněte se zadávání osobních údajů na webových stránkách, které používají pouze **protokol HTTP**.

Tipy

Zprávy HTTP jsou prostým textem, což znamená, že k nim přes internet mohou snadno přistupovat a číst je neoprávněné osoby. Protokol HTTPS přenáší všechna data v zašifrované podobě. Když uživatelé odesílají citlivé údaje, žádné třetí strany nemohou data přes síť zachytit.

2. Udržujte svůj software a operační systém aktuální

Pravidelně aktualizujte operační systém (OS), webový prohlížeč, antivirový software a další aplikace, abyste opravili známé zranitelnosti a chránili se před bezpečnostními hrozbami.

Tipy

Neodkládejte aktualizaci veškerého softwaru a aplikací, které používáte (osobně i pracovně), když obdržíte oznámení o aktualizaci. Pravidelně ověřujte, zda je vše aktuální v centru aplikací.

Co-funded by the European Union

4. Osvědčené postupy a správné návyky

4.2. Zabezpečené procházení

Při **procházení internetu dbejte** na dodržování následujících osvědčených postupů.

3. Používejte blokátory reklam a filtry obsahu

Nainstalujte si **blokátory reklam a filtry obsahu,** abyste zabránili škodlivým reklamám, vyskakovacím oknům nebo skriptům v ohrožení prohlížení nebo v přenosu malwaru. Některé webové stránky mohou pro přístup k obsahu vyžadovat jeho deaktivaci, kterou lze snadno provést pomocí ikony v prohlížeči.

Tipy

Nejlépe hodnocené bezplatné blokátory reklam:

- Původ uBlock
- Ochrana osobních údajů Badger
- Ghostery
- Adblock plus

4. Buďte opatrní při stahování

Stahujte software, soubory a přílohy pouze z **důvěryhodných zdrojů** a vyhněte se stahování obsahu z nedůvěryhodných webových stránek nebo neznámých zdrojů, abyste minimalizovali riziko napadení malwarem.

Tipy

Na internetu je k dispozici neuvěřitelné množství obsahu. Pokud nějaká webová stránka vyžaduje, abyste si něco stáhli, pravděpodobně se k podobnému obsahu dostanete z jiné webové stránky, aniž byste museli cokoli stahovat.

Co-funded by the European Union

4. Osvědčené postupy a správné návyky

4.2. Zabezpečené procházení

Při **procházení internetu dbejte** na dodržování následujících osvědčených postupů.

5. Anonymní prohlížení

Zvažte použití **virtuální privátní sítě (VPN),** abyste mohli **šifrovat** svůj internetový provoz a procházet anonymně, zejména při používání veřejných sítí Wi-Fi nebo při přístupu k citlivým informacím.

Tipy

Režim "inkognito" nebo "soukromé prohlížení" si nepleťte s VPN: nezajišťují větší bezpečnost prohlížení: pouze vymazávají historii prohlížení z vašeho zařízení. Historie prohlížení je však stále viditelná pro okolní svět, stejně jako vaše IP adresa, síť atd.

6. Pravidelně vymazávejte mezipaměť prohlížeče a soubory cookie

Pravidelně **vymazávejte** mezipaměť prohlížeče, soubory cookie a historii prohlížení, abyste odstranili **sledovací údaje** a minimalizovali riziko neoprávněného přístupu k vašim zvyklostem při prohlížení nebo osobním údajům.

Tipy

V prohlížeči Chrome klikněte na 3 tečky v pravém horním rohu > Odstranit data procházení. Na nově otevřené kartě vyberte období, za které chcete data vymazat (ideálně "Po celou dobu"), vyberte tři možnosti (historii procházení, soubory cookie a mezipaměť) a kliknutím na tlačítko "Odstranit data procházení" vymažte prohlížeč najednou.

Co-funded by the European Union

4. Osvědčené postupy a správné návyky

SociALL

4.3. Zabezpečené odesílání e-mailů

Při přijímání e-mailu si nezapomeňte položit následující otázky, abyste předešli jakémukoli bezpečnostnímu problému:

1. Znám a poznávám odesílatele?
2. Je e-mail neočekávaný nebo nevyžádaný?
3. Oslovuje mě e-mail jménem?
4. Jsou v textu pravopisné nebo gramatické chyby?
5. Existují podezřelé přílohy?
6. Obsahuje e-mail neočekávané odkazy?
7. Žádá e-mail o citlivé informace?
8. Vypadají podpis a kontaktní údaje důvěryhodně?
9. Mám s odesílatelem již nějaký vztah?
10. Používá e-mail výhrůžky nebo taktiku strachu?
11. Zjistil antivirový program něco podezřelého?
12. Vypadá stejně jako ostatní e-maily od tohoto poskytovatele?

Kromě toho dbejte na to, abyste k e-mailu vždy **přistupovali takto**:

- **Nikdy nepodnikejte okamžité, unáhlené kroky.**
- **Vždy předpokládejte,** že e-mail může být **podvodný,** věnujte čas jeho prostudování a "vymazání".
- **Důvěřujte svému úsudku** a instinktům: pokud se vám něco nezdá, prozkoumejte to opatrně.
- Nezapomeňte, že podvodníci hrají na **emoce,** jako je strach, zastrašování a vyhrožování. V každém případě zachovejte **chladnou hlavu** a **klid.**

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

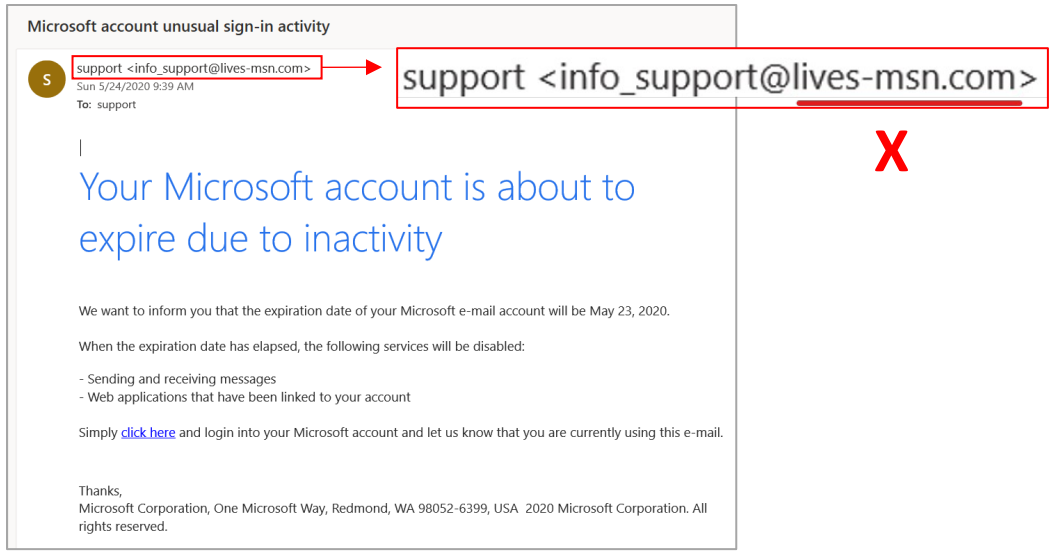
4. Osvědčené postupy a správné návyky

4.3. Zabezpečené odesílání e-mailů

Při přijímání e-mailu si nezapomeňte položit následující otázky, abyste předešli jakémukoli bezpečnostnímu problému:

1. Znám a poznávám odesílatele?

Ověřte si totožnost odesílatele, a to nejen zobrazením jména uvedeného nahoře a v podpisu, ale také **skutečnou e-mailovou adresou,** která e-mail odeslala.



X

2. Je e-mail neočekávaný nebo nevyžádaný?

Dávejte si pozor na nečekané e-maily, zejména na ty, které požadují **naléhavou akci** nebo nabízejí **nevyžádané služby**. Podvodníci je často používají k oklamání příjemců, nejčastěji s využitím těchto témat:

- Potřeba aktualizovat nebo ověřit informace o účtu (pozastavení účtu, vypršení platnosti, bezpečnostní upozornění atd.)
- Potřeba zaplatit čekající fakturu prostřednictvím odkazu
- Nabídky falešných pracovních příležitostí
- Platba nebo vzdálený přístup k počítači nebo účtu vyžádaný "podporou" za účelem řešení technických problémů.
- nutnost platit poplatky za zpracování nebo poskytovat osobní údaje za účelem získání nevyžádané odměny nebo ceny.

Co-funded by the European Union

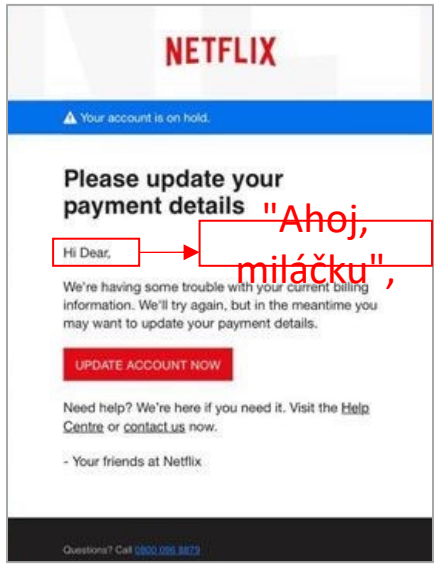
4. Osvědčené postupy a správné návyky

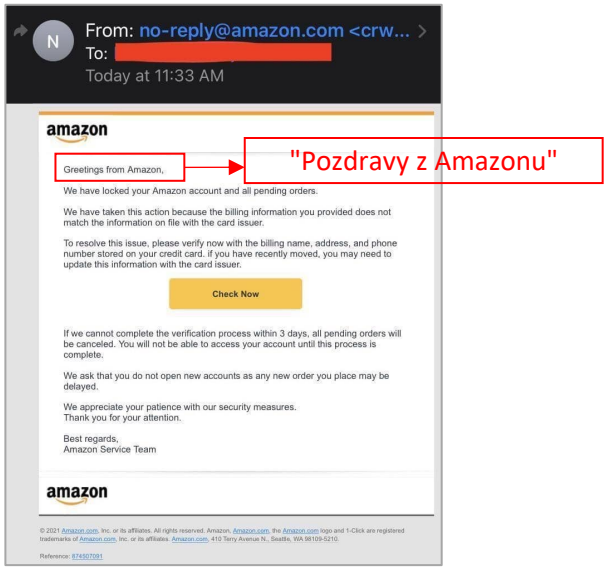
4.3. Zabezpečené odesílání e-mailů

Při přijímání e-mailu si nezapomeňte položit následující otázky, abyste předešli jakémukoli bezpečnostnímu problému:

3. Oslovuje mě e-mail jménem?

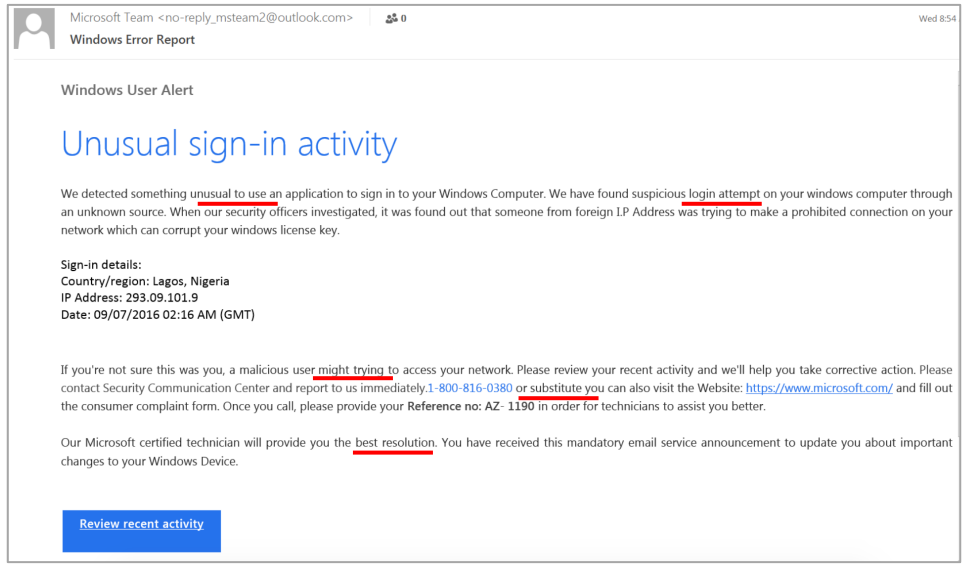
Legitimní organizace často používají ve své komunikaci vaše jméno. **Obecné pozdravy** nebo **chybné uvedení** vašeho jména mohou být varovným signálem.





4. Jsou v textu pravopisné nebo gramatické chyby?

Špatně napsané e-maily s **pravopisnými** nebo **gramatickými chybami** mohou znamenat pokus o phishing. Legitimní organizace obecně dělají ve svých e-mailech méně chyb.



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

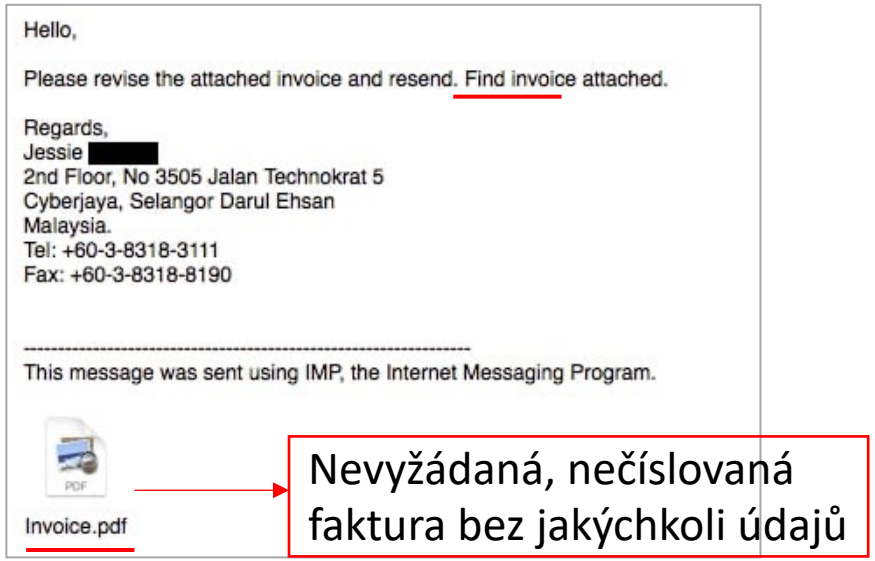
4. Osvědčené postupy a správné návyky

4.3. Zabezpečené odesílání e-mailů

Při přijímání e-mailu si nezapomeňte položit následující otázky, abyste předešli jakémukoli bezpečnostnímu problému:

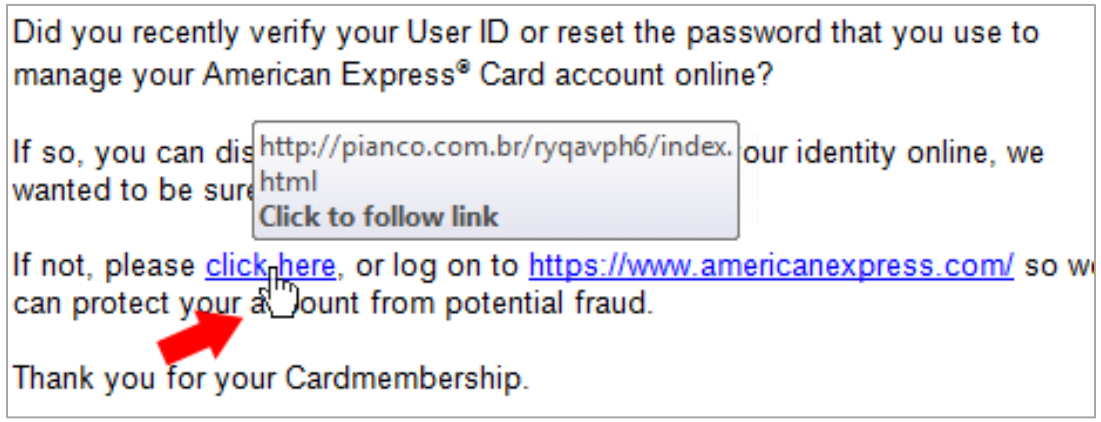
5. Existují podezřelé přílohy?

Vyvarujte se otevírání **neočekávaných příloh,** zejména z neznámých zdrojů. Škodlivé přílohy mohou obsahovat **malware** nebo pokusy o **phishing.**



6. Obsahuje e-mail neočekávané odkazy?

Pokud v e-mailu **najedete na** jakýkoli odkaz, aniž byste na něj klikli, zobrazí se **skutečná adresa URL**. Pokud se odkaz neshoduje s údajnou oficiální webovou stránkou odesílatele nebo vypadá podezřele, může se jednat o pokus o phishing.



JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
Medical car
åpenhet
Co-funded by the European Union

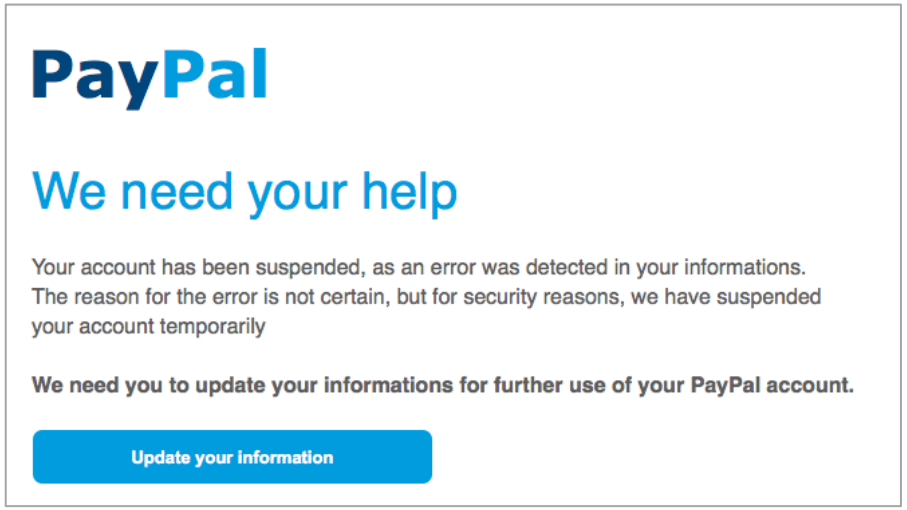
4. Osvědčené postupy a správné návyky

4.3. Zabezpečené odesílání e-mailů

Při přijímání e-mailu si nezapomeňte položit následující otázky, abyste předešli jakémukoli bezpečnostnímu problému:

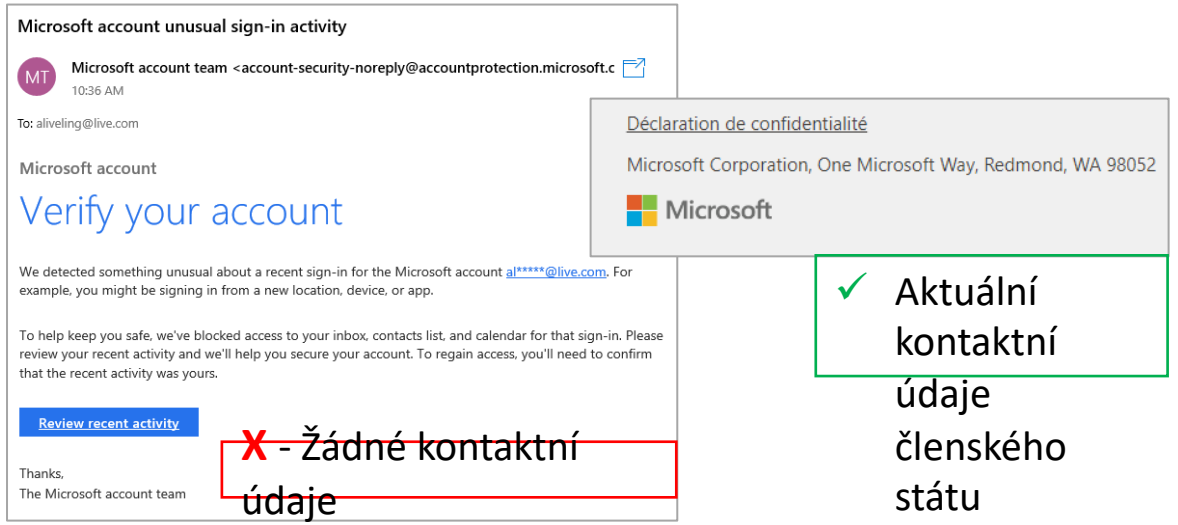
7. Žádá e-mail o citlivé informace?

Organizace obvykle **nevyžadují citlivé informace e-mailem** nebo prostřednictvím **odkazu** (například hesla nebo údaje o kreditní kartě), ale obvykle vás vyzvou k připojení k **účtu** na svých webových stránkách.



8. Vypadají podpis a kontaktní údaje důvěryhodně?

Legitimní organizace obvykle ve svých e-mailech uvádějí **jasné kontaktní údaje** včetně **fyzické adresy**. Ověřte si údaje odesílatele, včetně jeho **podpisu,** a porovnejte je s oficiálními zdroji.



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

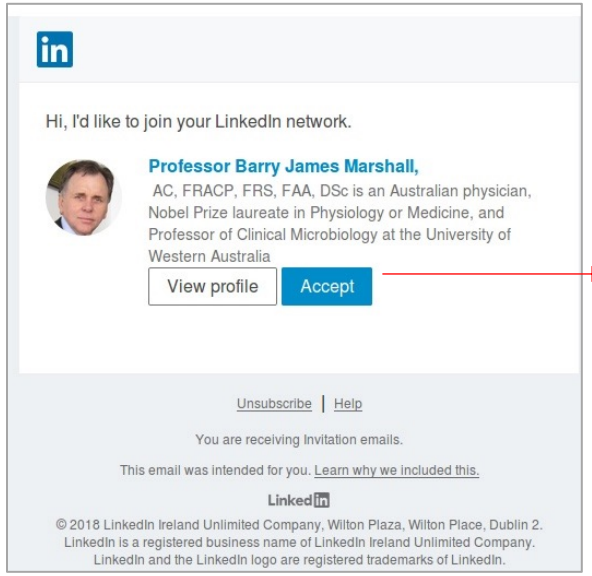
4. Osvědčené postupy a správné návyky

4.3. Zabezpečené odesílání e-mailů

Při přijímání e-mailu si nezapomeňte položit následující otázky, abyste předešli jakémukoli bezpečnostnímu problému:

9. Mám s odesílatelem již nějaký vztah?

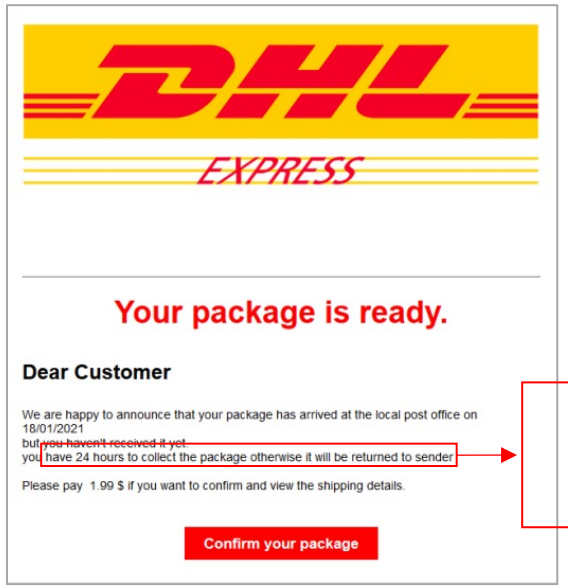
Pokud e-mail tvrdí, že pochází od organizace, u které máte účet, ověřte si informace raději **ve svém účtu,** než abyste se spoléhali pouze na e-mail.



Kontrola na účtu LinkedIn místo kliknutí na tlačítko "Přijmout"

10. Používá e-mail výhrůžky nebo taktiku strachu?

Podvodníci používají **výhrůžky**, **zastrašování** nebo taktiku **strachu**, aby příjemce přiměli k rychlému jednání. Dávejte si pozor na e-maily vyvolávající pocit **naléhavosti** nebo **strachu**.



"Na vyzvednutí zásilky máte 24 hodin, jinak bude vrácena odesílateli."

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

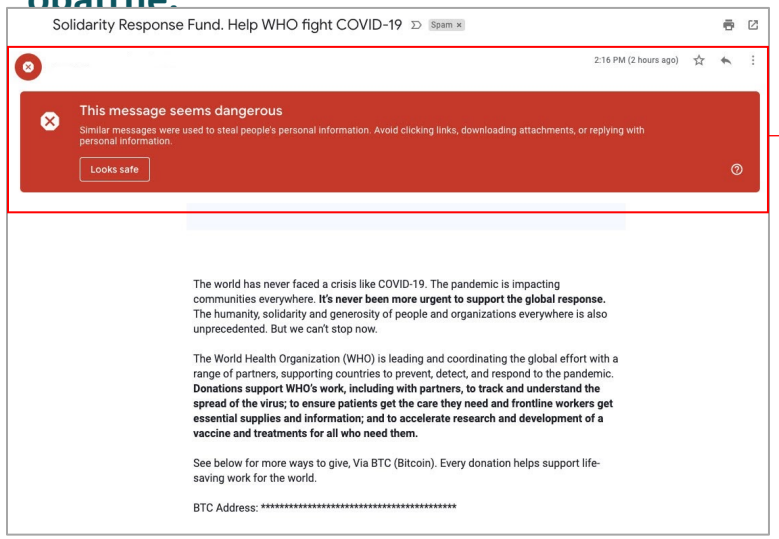
4. Osvědčené postupy a správné návyky

4.3. Zabezpečené odesílání e-mailů

Při přijímání e-mailu si nezapomeňte položit následující otázky, abyste předešli jakémukoli bezpečnostnímu problému:

11. Zjistil antivirový program něco podezřelého?

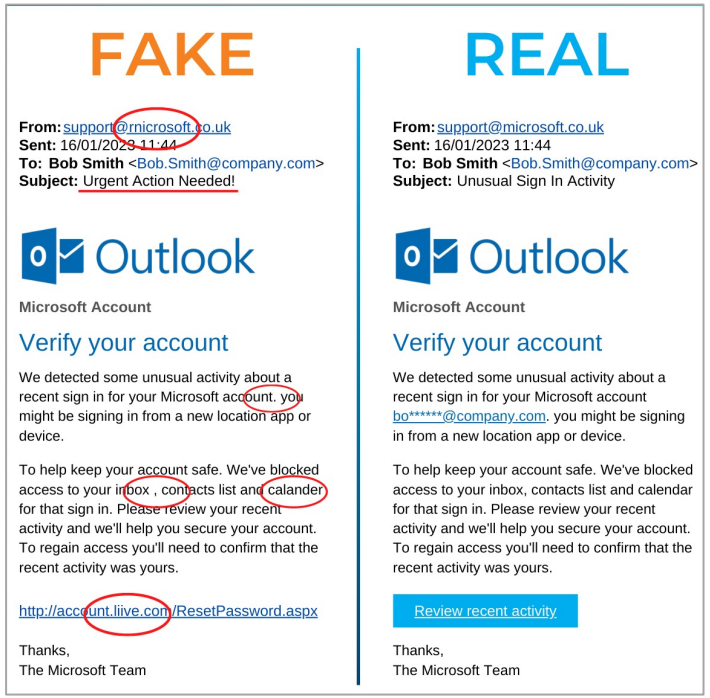
Většina poskytovatelů e-mailových služeb má **zabudované moduly pro** detekci pokusů o phishing. Kromě toho váš vlastní **antivirový program** mohl e-mail označit jako **podezřelý**. V takovém případě postupujte s e-mailem **opatrně**.



"Tato zpráva se zdá být nebezpečná"

12. Vypadá stejně jako ostatní e-maily od tohoto poskytovatele?

Pokud obdržíte e-mail pravděpodobně od organizace, od které **jste již e-maily obdrželi,** ověřte si, zda **se** design, značka, kontaktní údaje, autorská práva, odkazy a jazyk **shodují, a** teprve poté mu důvěřujte.



Co-funded by the European Union

4. Osvědčené postupy a správné návyky

4.4. Bezpečné používání sociálních médií

Bezpečně používejte sociální média, a to prostřednictvím následujících postupů.

1. Kontrola a úprava nastavení ochrany osobních údajů
2. Žádosti o přátelství a připojení si vybírejte
3. Pozor na phishing a podvody
4. Dávejte pozor na sdílení polohy a na to, co zveřejňujete.
5. Ověření pravosti účtu
6. Sledování aplikací a oprávnění třetích stran

Co-funded by the European Union

4. Osvědčené postupy a správné návyky

4.4. Sociální média a zasílání zpráv

Bezpečně používejte sociální média, a to prostřednictvím následujících postupů.

1. Zkontrolujte a upravte nastavení soukromí

Pravidelně **kontrolujte a upravujte nastavení soukromí na** platformách sociálních médií, abyste mohli kontrolovat, kdo může vidět vaše příspěvky, osobní údaje a fotografie.
Omezte okruh čtenářů svých příspěvků a zvažte **omezení přístupu k** citlivým informacím na důvěryhodné přátele a kontakty.

Tipy

Většina výchozích nastavení ochrany osobních údajů na sociálních sítích může umožnit sdílení vašich informací s jinými online uživateli třetích stran, včetně vašeho jména, věku, místa bydliště, pohlaví atd.

2. Žádosti o přátelství a připojení si vybírejte

Buďte opatrní při přijímání **žádostí o přátelství nebo připojení** od neznámých osob. Před přijetím žádosti si ověřte totožnost dané osoby, zejména pokud ji osobně neznáte.
Mnoho podvodníků na sociálních sítích začíná tím, že se stanou "vašimi přáteli" a získají **přístup k dalším vašim údajům**.

Tipy

Pokuste se ověřit pravost žádosti jinými prostředky. Například: pokud obdržíte žádost od někoho, kdo tvrdí, že je bratr vašeho přítele, můžete svého přítele požádat, aby před přijetím žádosti potvrdil totožnost této osoby.

Co-funded by the European Union

4. Osvědčené postupy a správné návyky

4.4. Sociální média a zasílání zpráv

Bezpečně používejte sociální média, a to prostřednictvím následujících postupů.

3. Pozor na phishing a podvody

Buďte **obezřetní vůči nevyžádaným** zprávám, odkazům nebo žádostem od neznámých osob na sociálních sítích. **Vyvarujte se klikání na podezřelé odkazy** nebo stahování příloh z neznámých zdrojů, protože mohou vést k phishingovým podvodům nebo infekci malwarem.

Tipy

K mnoha podvodům na sociálních sítích dochází nabouráním se do účtu některého z vašich kontaktů. Buďte obezřetní, když vám známý kontakt pošle nevyžádané, neobvyklé žádosti (například o finanční podporu pro své příbuzné v nemocnici), a ověřte si to u něj prostřednictvím jiného média.)

4. Dávejte pozor na sdílení polohy a na to, co zveřejňujete.

Omezte sdílení polohy na platformách sociálních médií, zejména při zveřejňování fotografií nebo aktualizací v reálném čase. Vyvarujte se zveřejňování své přesné polohy nebo sdílení osobních údajů, které by mohly ohrozit vaši bezpečnost.

Tipy

Kyberzločinci mohou ke způsobení škody využít mnoho typů informací. Kromě zřejmých údajů (jméno, věk, pohlaví, město bydliště atd.) mohou kyberzločinci využít i mnoho dalších údajů, například název nejbližší školy, bývalé nebo současné pracoviště, snímky obrazovky s osobními údaji atd.

Co-funded by the European Union

4. Osvědčené postupy a správné návyky

4.4. Sociální média a zasílání zpráv

Bezpečně používejte sociální média, a to prostřednictvím následujících postupů.

5. Ověření pravosti účtu

Dávejte si pozor na **falešné nebo vydávané účty na** platformách sociálních médií, zejména na ty, které se vydávají za celebrity, veřejně známé osoby nebo značky. Před interakcí s účty nebo sdílením osobních údajů **si ověřte** jejich **pravost.**

Tipy

Jen v roce 2021 Facebook odstranil 1,7 miliardy falešných účtů. Stejně tak téměř 1 z 5 (19,42 %) účtů na Twitteru je falešný nebo spam. Modré zaškrtnutí "certifikující" účet může získat prakticky kdokoli a není ukazatelem toho, že účtu lze důvěřovat.

6. Sledování aplikací a oprávnění třetích stran

Pravidelně **kontrolujte a spravujte** oprávnění udělená aplikacím třetích stran připojeným k účtům sociálních médií. Odeberte přístup aplikacím, které již nepoužíváte nebo jim nedůvěřujete, abyste minimalizovali riziko zneužití dat nebo narušení soukromí.

Tipy

Dávejte pozor na oprávnění těchto aplikací, protože by mohly umožnit přístup k soukromým informacím, ke kterým by neměly mít přístup.

Co-funded by the European Union

4. Osvědčené postupy a správné návyky

SociALL

4.5. Zabezpečení mobilních zařízení

Používejte své **mobilní zařízení bezpečněji, pokud** zavedete následující postupy.

1. Použití bezpečného zámku obrazovky
2. Udržujte svůj software a operační systém aktualizovaný
3. Šifrování dat
4. Použití důvěryhodného obchodu s aplikacemi
5. Přezkoumání oprávnění aplikace
6. Dávejte si pozor na veřejnou Wi-Fi
7. Povolení funkce "Najít mé zařízení"
8. Omezení používání Bluetooth a NFC

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.
MPWA
Medicalscar
åpenhet
Co-funded by the European Union

4. Osvědčené postupy a správné návyky

4.5. Zabezpečení mobilních zařízení

Používejte své **mobilní zařízení bezpečněji, pokud** zavedete následující postupy.

1. Používejte bezpečný zámek obrazovky

Povolte **bezpečný zámek obrazovky (např.** PIN, heslo, vzor, biometrická identifikace), abyste zabránili neoprávněnému přístupu k zařízení v případě jeho ztráty nebo krádeže. Vyvarujte se používání snadno uhodnutelných vzorů nebo kódů PIN.

2. Udržujte svůj software a operační systém aktualizovaný

Pravidelně **aktualizujte mobilní operační systém**, aplikace a bezpečnostní záplaty, abyste se chránili před známými zranitelnostmi a bezpečnostními hrozbami. Povolte automatické aktualizace, abyste zajistili včasné bezpečnostní záplaty.

3. Šifrování dat

Povolte šifrování dat uložených v mobilním zařízení, abyste ochránili citlivé informace. Většina moderních mobilních zařízení nabízí vestavěné funkce šifrování, které šifrují data v klidovém stavu.

4. Používejte důvěryhodný obchod s aplikacemi

Stahujte aplikace pouze z **oficiálních a důvěryhodných obchodů s aplikacemi, jako je** Apple App Store nebo Google Play Store, abyste minimalizovali riziko stažení škodlivých aplikací nebo malwaru.

Co-funded by the European Union

4. Osvědčené postupy a správné návyky

4.5. Zabezpečení mobilních zařízení

Používejte své **mobilní zařízení bezpečněji, pokud** zavedete následující postupy.

5. Zkontrolujte oprávnění aplikace

Zkontrolujte a spravujte oprávnění aplikací, abyste mohli kontrolovat, k jakým datům a funkcím mají aplikace v zařízení přístup. **Zakázat nepotřebná oprávnění, která** aplikace pro svou funkčnost nepotřebují.

6. Buďte obezřetní na veřejných Wifi

Vyhněte se připojování k **nezabezpečeným veřejným sítím Wi-Fi,** protože mohou být náchylné k odposlechu nebo útokům typu man-in-the-middle. Při připojování k veřejným sítím Wi-Fi **používejte k** šifrování internetového provozu **síť VPN.**

7. Povolte funkci "Najít mé zařízení"

Povolte na svém mobilním zařízení funkci "**Najít mé zařízení"** nebo "**Najít můj iPhone",** abyste mohli své zařízení na dálku lokalizovat, uzamknout nebo vymazat v případě jeho ztráty nebo krádeže. Tato funkce pomáhá chránit vaše data a soukromí v případě krádeže nebo ztráty.

8. Omezte používání Bluetooth a NFC

Pokud **Bluetooth a NFC** nepoužíváte, **vypněte je,** abyste zabránili neoprávněnému přístupu nebo párování s jinými zařízeními. Při párování s neznámými zařízeními buďte opatrní a používejte zařízení Bluetooth z důvěryhodných zdrojů.

Co-funded by the European Union

4. Osvědčené postupy a správné návyky

4.6. Zabezpečení heslem

Zabezpečte svá hesla tak, aby obsahovala následující prvky.

1. Používejte silná a jedinečná hesla
2. Pro každý účet používejte jiná hesla
3. Používejte spíše přístupové fráze než slova
4. Použití renomovaného správce hesel
5. Vždy uchovávejte hesla v tajnosti
6. Pravidelná aktualizace hesel

Co-funded by the European Union

4. Osvědčené postupy a správné návyky

4.6. Zabezpečení heslem

Zabezpečte svá hesla tak, aby obsahovala následující prvky.

1. Používejte silná a jedinečná hesla

Vytvářejte silná a složitá hesla, která je obtížné uhodnout. Používejte kombinaci velkých a malých písmen, číslic a speciálních znaků. Nepoužívejte snadno uhodnutelné informace, jako jsou jména, data narození nebo běžná slova.

Tipy

Některé weby poskytují informaci o zabezpečení hesla. Heslo neregistrujte, dokud jej webová stránka nebo software nevyhodnotí jako "silné". Hesla by měla mít alespoň 16 znaků a kombinovat různé typy znaků.

2. Pro každý účet používejte jiná hesla

Nepoužívejte stejné heslo pro více účtů. Pro každý online účet používejte jedinečná hesla, abyste minimalizovali dopad narušení bezpečnosti na ostatní účty.

Tipy

Používejte správce hesel, abyste si nemuseli pamatovat nebo zapisovat hesla. Budete si muset pamatovat pouze heslo ke správci hesel.

Co-funded by the European Union

4. Osvědčené postupy a správné návyky

4.6. Zabezpečení heslem

Zabezpečte svá hesla tak, aby obsahovala následující prvky.

3. Používejte spíše hesla než slova

Zvažte používání **přístupových frází namísto** tradičních hesel. Hesla jsou delší **kombinace slov nebo frází, které** jsou snadněji zapamatovatelné, ale hůře prolomitelné. Silnou heslovou frází je například "Icàre@b0utSecur1ty!".

Tipy

Nejprve si zvolte přístupovou frázi, kterou si snadno zapamatujete. Pak si vytvořte vlastní "šifrovací systém", například: o=0, i=1, a=@ atd. Dbejte na to, abyste do hesla začlenili také velká písmena a speciální znaky.

4. Používejte renomovaného správce hesel

K bezpečnému ukládání a správě hesel používejte **renomovaného správce hesel.** Správci hesel generují silná, jedinečná hesla pro každý účet a ukládají je do šifrovaného trezoru, který je přístupný pouze s hlavním heslem.

Tipy

Příklady renomovaných správců hesel jsou uvedeny v poslední části tohoto učebního plánu. Nezapomeňte použít funkci generování hesel, abyste mohli využívat jedinečná, silná a náhodně generovaná hesla, která si nemusíte pamatovat.

Co-funded by the European Union

4. Osvědčené postupy a správné návyky

4.6. Zabezpečení heslem

Zabezpečte svá hesla tak, aby obsahovala následující prvky.

5. Vždy udržujte hesla v tajnosti

Nikdy nikomu nesdělujte svá hesla, včetně přátel, členů rodiny nebo kolegů. Udržujte svá hesla v tajnosti a nezapisujte si je ani je neukládejte na snadno přístupných místech. Ujistěte se, že jsou uložena ve správci hesel.

Tipy

Pokud je sdílení hesla nevyhnutelné, udělejte to raději ústně, případně prostřednictvím zabezpečené šifrované aplikace (např.: nikdy ne přes sociální sítě). Nikdy nesdílejte přihlašovací jméno / e-mailovou adresu prostřednictvím stejné aplikace, a to prostřednictvím jiného média.

6. Pravidelně aktualizujte hesla

Pravidelně aktualizujte hesla k online účtům, zejména k citlivým účtům, jako jsou bankovní účty, e-mailové účty nebo účty sociálních médií. Pokud máte podezření, že hesla mohla být prozrazena, okamžitě je změňte a nechte správce hesel pravidelně generovat nová hesla.

Tipy

Nezapomeňte změnit výchozí hesla dodávaná se zařízeními, směrovači nebo softwarovými aplikacemi. Výchozí hesla jsou často snadno uhodnutelná a všeobecně známá, což je činí zranitelnými vůči neoprávněnému přístupu.

Co-funded by the European Union

SociALL

5. Užitečné nástroje a další zdroje

1. Správci hesel
2. Nástroje 2FA
3. Anti malwares
4. Šifrovací nástroje
5. Další nástroje

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

5. Užitečné nástroje a další zdroje

5.1. Správci hesel

SociALL

LastPass

1Password

NordPass®

KEEPER®

Správci hesel **bezpečně ukládají a spravují hesla k** různým účtům, zjednodušují přístup a zároveň zajišťují vytvoření silného a jedinečného hesla a bezpečný přístup. Ujistěte se, že:

- **Zvolte si silné, jedinečné a zapamatovatelné hlavní heslo**, které vám umožní přístup ke správci hesel. Určitě si ho zapamatujte a nikdy ho nesdělujte; je to vstupní brána ke všem vašim účtům.
- **Nechte správce hesel vygenerovat silná a jedinečná hesla** pro každý z vašich účtů. Zapamatuje si je a uloží a vy nikdy nebudete mít stejné heslo dvakrát.

JIHOMĚSTSKÁ SOCIÁLNÍ a.s.

MedicalScan

åpenhet

Co-funded by the European Union

5. Užitečné nástroje a další zdroje

5.2. Nástroje dvoufaktorového ověřování (2FA)

Nástroje dvoufaktorového ověřování (2FA) zvyšují zabezpečení účtu tím, že nutí uživatele ověřit své přihlášení na dvou různých registrovaných a důvěryhodných zařízeních, obvykle na telefonu a počítači.

5. Užitečné nástroje a další zdroje

5.3. Anti-malware

Antimalwarové programy nebo antiviry identifikují a odstraňují různé typy malwaru a poskytují zařízením a sítím ochranu před kybernetickými hrozbami v reálném čase.

5. Užitečné nástroje a další zdroje

5.4. Šifrovací nástroje

Šifrovací nástroje vytvářejí šifrované kontejnery, které chrání citlivé soubory a složky tím, že zabraňují neoprávněnému přístupu pomocí šifrování. Některé nástroje, například Bitlocker, šifrují externí periferní zařízení, jako je pevný disk, a zvyšují tak jejich zabezpečení.

Co-funded by the European Union

5. Užitečné nástroje a další zdroje

5.5. Další užitečné nástroje

Název	Typ	Popis
Ochrana osobních údajů Badger	Rozšíření prohlížeče	Nástroj Privacy Badger blokuje sledovací soubory cookie a reklamy a chrání soukromí uživatele tím, že brání sledovacím zařízením třetích stran ve shromažďování údajů o prohlížení.
Imprivata	Správa přístupu	Společnost Imprivata nabízí řešení jednotného přihlášení, které umožňuje pracovníkům v oblasti péče bezpečný přístup k více aplikacím pomocí jediného přihlášení, čímž se zefektivní pracovní postupy bez ohrožení bezpečnosti.
HIPAA One	Nástroj pro dodržování předpisů	HIPAA One automatizuje dodržování předpisů HIPAA a pomáhá zdravotnickým organizacím plnit regulační požadavky, provádět hodnocení rizik a zajišťovat bezpečnost dat.
Ochrana koncových bodů společnosti Symantec	Zabezpečení koncových bodů	Symantec Endpoint Protection nabízí komplexní zabezpečení včetně pokročilé ochrany před hrozbami, antivirového programu a brány firewall, které chrání před kybernetickými hrozbami ve zdravotnických zařízeních.
TeamViewer	Vzdálený přístup k ploše	TeamViewer umožňuje vzdálený přístup k zařízením a jejich ovládání, což napomáhá vzdálené technické podpoře, řešení problémů a spolupráci na různých místech.
Cisco AnyConnect	Nástroj VPN	Cisco AnyConnect poskytuje zabezpečené připojení VPN, které umožňuje šifrovaný přístup do sítí organizace ze vzdálených míst a chrání přenosy dat.
Adobe Sign	Platforma pro elektronický podpis	Adobe Sign usnadňuje bezpečné digitální podepisování dokumentů, zjednodušuje a urychluje proces podepisování a zajišťuje soulad s předpisy a bezpečnost při správě dokumentů.

Děkujeme za vaši účast a nápady!

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