

ŘEŠENÍ PRACOVNÍCH LISTŮ

1) BEZPEČNÁ PRÁCE S HESLY

1. Jaká existují pravidla pro vytváření silného bezpečného hesla?

Je dlouhé minimálně 12 znaků.

Nemá „význam“ spojitost s něčím reálným (např. jména).

Obsahuje malá i velká písmena a číslice.

Obsahuje speciální znaky.

2. Uveďte příklady silných a slabých hesel:

Silná hesla: Např. **NejHok97?Flor**

Slabá hesla: Např. **Admin, 123456**

3. Proč je důležité mít pro každý účet jiné heslo?

Minimalizuje se tím únik hesla, pokud dojde k prolomení databáze přihlašovacích údajích na nějakém webu, kde jsme registrovaní.

4. Co je správce hesel?

Uchovává a spravuje hesla pro různé weby, dokáže vygenerovat heslo pro každý jednotlivý web jiné.

5. Z čeho se skládá dvoufázové ověření?

Login/přihlašovací údaje + mobilní autentifikátor, biometrické údaje apod.

6. Uveďte výhody a nevýhody správce hesel:

Příklady:

Výhody: Vytváření silných hesel, pro každý web/aplikaci jiné. Jednoduché použití, centralizované uložení, synchronizace na různých zařízeních.

Nevýhody: Jsou závislé na jednom hesle (pokud dojde k prolomení, přijdeme o všechna hesla). Pokud nemáme instalovaný správce hesel na zařízení musíme opisovat dlouhá hesla ze správce hesel, abychom se mohli přihlásit.

2) ÚTOKY – CÍLE A METODY ÚTOČNÍKŮ

1. Přiřad'te správný pojem k definici:

- Malware (Spyware)-** Škodlivý software, který může být použit k infikování počítačů nebo mobilních zařízení s cílem získat citlivé informace.
- Skimming -** Zařízení umístěné na bankomatu nebo platebním terminálu, které umožňuje získat informace z kreditní karty.
- Phishing -** Útok, který se pokouší ukrást citlivá data tak, že vás přiměje odhalit osobní údaje na podvrhnutých webových stránkách.
- Ransomware -** Zablokuje přístup k počítači a požaduje výkupné.

2. Jaké jsou typické znaky phishingových e-mailů?

- Špatná čeština
- Zvláštní telefonní čísla a emaily
- Nabídka nereálných sum.
- Vyžadování odeslání osobních údajů.
- Nátlak na posláni peněz.

3. Jak byste reagovali na podezřelou zprávu nebo email?

- Určitě neklikali na URL adresy obdržené v emailu.
- Pokud bychom si opravdu nebyli jisti zaslání emailu s dotazem na oficiální email společnosti, zda se jedná o reálný email.
- Zablokovat si telefonní číslo a email.

4. Uved'te, co je na obrázcích níže podezřelé?

- Podezřelé telefonní číslo, neoficiální odkaz instituce, špatná diakritika
- Podezřelý email, vyžaduje zaslání osobních údajů, vyhrožuje smyšlenou exekucí, nereálná částka, kterou bychom měli dostat (typický scam).

3) SOCIÁLNÍ INŽENÝRSTVÍ

1. Proč je důležité chránit své osobní údaje online?

Aby nám nebyly odcizeny/zneužity podvodníkem.

Aby se za nás nemohl nikdo s našimi osobními údaji vydávat.

2. Jaké osobní údaje by neměly být sdíleny?

Datum narození, rodné číslo, fotka občanského průkazu/pasu, adresa bydliště, přihlašovací údaje, hesla apod.

3. Vysvětlete pojem Sociální inženýrství:

Sociální inženýrství je technika, která zahrnuje manipulaci s lidským chováním a důvěrou, aby se získaly citlivé informace nebo přístup k systémům.

4. Vysvětlete následující metody/techniky sociálního inženýrství:

Pretexting: Vytváření falešného příběhu nebo scénáře k získání důvěry a citlivých informací od oběti.

IVR (*telefonní phishing*): Útoky prováděné přes interaktivní hlasové odpovědi. Osoba volá na falešné číslo společnosti a hlasový automat si vyžádá přístupové/osobní údaje.

Baiting: Útočník nechá infikovaná přenosná média na místech, kde je někdo s velkou pravděpodobností najde. Po použití např. flashdisku se do počítače nainstaluje vir.

Quid pro quo (*něco za něco*): Volání na náhodná čísla společnosti. Útočník se vydává za pracovníka technické podpory. Pokud najde nespokojeného zaměstnance vyžádá si instalaci software, přes který se dostane do počítače i firemní sítě.

5. Jak se můžeme chránit před technikami sociálního inženýrství?

Nesdílet osobní informace s neznámými osobami online nebo přes telefon.

Ověřovat si totožnost lidí, se kterými komunikujeme.

Před otevřením odkazu v konverzaci zkontrolovat, zda odkaz odpovídá oficiálním stránkám.

4) DIGITÁLNÍ STOPA

1. Vysvětlete pojem digitální stopa:

Digitální stopa jsou informace, které zanechává online prostřednictvím našich aktivit na internetu. Ve většině případů o tom ani vůbec nevíme.

2. Zakroužkujte pojmy, které jsou součástí digitální stopy.

Příspěvky na sociálních sítích, historie nákupů, platební údaje, komentáře, historie vyhledávání, e-mailová komunikace, poloha a geolokační data.

3. Jak může naše digitální stopa ovlivnit naše soukromí a bezpečnost?

Ztráta soukromí – Může odhalit osobní informace a soukromý život uživatelů

Cílená reklama – Firmy využívají pro cílenou reklamu a personalizované nabídky

Riziko kybernetických útoků – Útočníci mohou využít informace k provedení phishingových útoků, Krádeže identity, Únik dat

4. Co můžeme udělat pro ochranu soukromí a minimalizaci digitální stopy?

Omezení sdílení osobních informací

Používat bezpečná hesla

Kontrola nastavení soukromí na sociálních sítích

Omezit sdílení soukromých informací

Využívat anonymní okna při vyhledávání informací

5. Dají se data, která jsme zveřejnili online smazat?

Velmi obtížně, proto je důležité přemýšlet o tom, co online zveřejňujeme.

6. Zhodnoťte svoji současnou digitální stopu:

K zamyšlení: Změníte některé své návyky v chování na internetu?

5) ZABEZPEČENÍ DIGITÁLNÍCH ZAŘÍZENÍ A DAT

1) Vypište alespoň 3 opatření, které můžete udělat nejen pro fyzické zabezpečení počítačů ve vašem domě nebo školním prostředí.

Např.:

Nenechávat zařízení bez dozoru

Použití zámků a bezpečnostních kabelů na veřejnosti

Chráněný vstup do budovy

Pravidelné aktualizace

2) K čemu slouží Sandbox programy?

Využívané ke spouštění neznámých a potenciálně nebezpečných aplikací

Nedojde k poškození vašeho počítače

3) Jak funguje firewall?

Slouží k řízení síťového provozu

Definuje pravidla pro komunikaci mezi sítěmi

Odděluje sítě

4) Jakých chyb se může uživatel dopustit při práci s počítačem?

Neaktualizovaný software

Nesprávná manipulace se soubory

Nedostatečná záloha dat

Otevírání neznámých příloh a odkazů

5) Najděte žebříček nejlépe hodnocených antivirů a vypište první 3.

Např.: <https://www.webhostingcentrum.cz/nejlepsi-antiviry/>

Bitdefender, Norton 360, Avast Ultimate

6) ŠIFROVÁNÍ DAT

1) K čemu se šifrování dat používá a proč je důležité?

Slouží k ochraně dat, proti nežádoucímu přístupu cizích osob.

Chrání citlivá data před zneužitím a zajišťuje jejich bezpečný přenos a uchovávání.

2) Máte zkušenosti s používáním šifrování dat?

3) Jaký je rozdíl mezi symetrickým a asymetrickým šifrováním?

Symetrické

Asymetrické

Rychlé

Pomalejší

Méně náročné na výpočty

Náročnější na výkon

Méně bezpečné

Více bezpečné

Jeden klíč na šifrování i dešifrování

Dva klíče (veřejný, privátní)

4) Pomocí Caesarovy šifry zašifrujte tato slova:

auto ⇒ **bvup**

predmet ⇒ **qsfenfu**

_____ ⇒ _____

5) Pomocí caesarovy šifry dešifrujte tato slova:

prazdniny ⇐ qsbaojoz

hora ⇐ ipsb

jednicka ⇐ kfeojdlb

7) ZÁLOHOVÁNÍ A ARCHIVACE DAT

1) Je rozdíl mezi archivací a zálohováním? Pokud ano jaký?

Zálohování dat je kopie dat sloužící k rychlé obnově dat v případě ztráty nebo poškození.

Archivace je přesun důležitých dat z hlavního úložiště na archivační médium. Pro použití v budoucnu.

2) Vyjmenuje alespoň 4 možnosti, kde můžete ukládat data:

Pevný disk

Cloud

NAS

Přenosný disk

Flash disk

CD

3) Jaké jsou zásady při zálohování:

Pravidelně ukládat data

Kontrolovat zálohy (zda nejsou poškozené)

Ukládání záloh na různá místa

Využívat automatické zálohování