Internetová rizika a jak je poznat

Internet nabízí spoustu možností – od studia přes komunikaci až po práci.
Zároveň je ale i místem, kde číhají různé nástrahy: podvodné e-maily, škodlivé odkazy nebo viry. Stačí chvilka nepozornosti a vaše data, hesla či zařízení mohou být v ohrožení.

Na této stránce najdete přehled těch nejčastějších typů útoků, jak je poznat a jak se jim vyhnout. Aktuální varování před útoky, doporučení a přehled typických podvodů najdete v sekci Aktuální hrozby ÚVT .

Phishing - když vám někdo "háže návnadu"

Nejčastěji se podvodníci vydávají za univerzitu, banku, dopravní službu nebo jinou důvěryhodnou instituci. Cílem je vylákat z vás přihlašovací údaje, číslo karty nebo jiné citlivé informace.
Jak Phishing poznáte?
- Zpráva na vás tlačí k okamžité akci (např. "obnovte účet", "klikněte ihned" nebo "hrozí zablokování").
- Odkaz vede na podezřelou nebo neznámou adresu - často se jen nepatrně liší (např. cuni-login.net místo cuni.cz)
- Zdánlivě oficiální e-mail obsahuje gramatické chyby, podivné fráze nebo logické nesmysly.
- Odesílatel chce vaše heslo, číslo karty nebo jiné soukromé údaje.

Nejčastější typy
- email
- SMS zpráva
- sociální sítě

Jak se bránit?
- Nikdy neklikejte na odkazy v podezřelých e-mailech.
- Hesla nezadávejte mimo oficiální přihlašovací stránky.
- Nikdy nikomu nesdělujte své heslo.
- Pokud si nejste jistí, přepošlete e-mail fakultní podpoře - raději ověřit, než litovat.

Malware - viry, spyware, ransomware

Malware je škodlivý software, který se může dostat do vašeho zařízení s cílem ho poškodit nebo ukrást data.
Nejčastější typy
- **Viry** - šíří se přes infikované soubory, flash disky nebo přílohy e-mailů.
- **Spyware** - sleduje co děláte, sbírá údaje a data odesílá útočníkům.
- **Ransomware** - zamkne vaše soubory a požaduje výkupné za jejich odemčení.

Jak se chránit?
- Používejte **aktuální antivirový program** a mějte zapnuté automatické aktualizace.
- Neinstalujte programy z neznámých webů.
- Neotevírejte přílohy od lidí, které neznáte - ani když to "vypadá důvěryhodně".

Spam - nevyžádaná pošta

Spam jsou nevyžádané e-maily, které mohou obsahovat obtěžující reklamu, odkazy na podvodné weby nebo škodlivé přílohy.
Jak ho poznat?
- podezřelá adresa odesílatele nebo nesmyslná doména
- pravopisné chyby a neobvyklé formulace
- odkazy, které při najetí myší vedou na jinou adresu, než jaká je viditelná

Jak s ním naložit?
- Spam neotvírejte, nemažte ručně – použijte funkci „Označit jako spam“.
- Nikdy nereagujte a neklikejte na odkazy „odhlásit odběr“, pokud si nejste jistí, odkud e-mail pochází.
- Aktualizujte filtry nevyžádané pošty – většina e-mailových služeb to dělá automaticky.

Podvodné přílohy

Nikdy neotvírejte přílohy od neznámých odesílatelů, obsahují škodlivý software. Slouží k instalaci malwaru, ransomwaru nebo krádeži údajů.
Jak je poznat?
- Obsahují podezřelé přípony: .exe, .scr, .rar, .vbs nebo zdvojené jako .pdf.exe.
- Neočekávaná zpráva: přišel dokument, který jste neobjednali/neočekávali
- Nátlak: hrozba exekuce, odpojení služeb

Co dělat při podezření?
- **Neotvírat**: přílohu nestahuje a na nic neklikejte.
- **Ověřit**: kontaktujte odesílatele jiným způsobem (např. telefonicky)
- **Nahlásit/Smazat**: E-mail nahlaste jako phishing a smaže.
- **Zabezpečit**: pokud jste přílohu otevřeli, spusťte antivirovou ochranu.

Falešné webové stránky

Vypadají jako originál, ale kradou data.
Ve skutečnosti jsou navrženy jen proto, abyste do nich zadali své přihlašovací údaje, které pak útočník okamžitě získá.
Jak je poznat?
- Podezřelá URL adresa: často se liší jen v jednom písmenku nebo doméně.
- Chybějící https a certifikáty: ikona visacího zámku v adresním řádku značí šifrování.
- Jazykové chyby: částým znakem jsou špatná čeština a gramatické chyby.
- Chybějící kontakty: podvodný web nemá zájem o komunikaci, není uvedeno telefonní číslo ani sídlo firmy.

Podvodné soutěže a investiční nabídky

„Vyhráli jste nový iPhone!“ nebo „Zhodnoťte své úspory o 500 % během týdne!“ Zní to lákavě – ale ve skutečnosti jde téměř vždy o podvod.
Jak se nenechat nachytat?
- Pokud je nabídka „až příliš dobrá, aby byla pravda“, většinou pravda není.
- Nikdy neposílejte peníze ani osobní údaje neznámým subjektům.
- U e-shopů si vždy ověřte, že používají zabezpečené připojení (https://) a mají reálné kontaktní údaje.

Sociální inženýrství - když vás útočník manipuluje

Ne všechny útoky jsou technické – často útočník zneužívá naši důvěřivost nebo snahu pomoci.
Jak to vypadá?
- Někdo vám zavolá a tvrdí, že je z IT podpory – a potřebuje vaše heslo.
- Někdo se vydává za vedoucího/kolegu, který „rychle potřebuje" přístup k dokumentu.
- Dostanete e-mail s logem univerzity a výzvou ke „kontrole účtu“.

Jak reagovat?
- Nikdy neposkytujte heslo, PIN ani jiné přístupové údaje – IT podpora je po vás NIKDY chtít nebude.
- Pokud si nejste jistí, ověřte si situaci oficiální cestou (telefonicky, osobně nebo přes univerzitní e-mail).

Potřebujete poradit nebo nahlásit bezpečnostní incident?

Podrobný postup najdete v sekci Hlášení bezpečnostního incidentu , kde se dozvíte, jak incident popsat, komu ho zaslat a jak probíhá řešení.

Často kladené dotazy (FAQ)
Dostal/a jsem e-mail s logem UK, ale něco mi na něm nesedí. Co mám dělat?
- Zkontrolujte adresu odesílatele. Pokud nekončí na @cuni.cz nebo působí podezřele, e-mail neotvírejte a nahlaste ho IT podpoře.

Jak poznám falešnou webovou stránku?

- Zkontrolujte adresu – měla by začínat https:// a patřit do domény .cuni.cz nebo jiné oficiální domény instituce.

Mám kliknout na odkaz pro „obnovení účtu“, který mi přišel e-mailem?

- Ne! Nikdy nezadávejte své přihlašovací údaje přes odkazy v e-mailech. Přihlašujte se vždy ručně přes oficiální web UK.

Co dělat, když jsem klikl/a na podezřelý odkaz nebo otevřel/a přílohu?

- Okamžitě odpojte zařízení od internetu, spusťte antivirovou kontrolu a kontaktujte IT podporu.

Jak zabránit tomu, aby mi chodilo tolik spamu?

- Používejte univerzitní e-mail a nepište svou adresu veřejně na weby či fóra.
- Nevyplňujte formuláře na neověřených stránkách a využívejte spamové filtry.

Jak se bránit internetovým útokům v 5 bodech
Kontrolujte, odkud zprávy přicházejí
Ověřte adresu odesílatele – pokud je to podle jména váš kolega, ale adresa ve skutečnosti nekončí cuni.cz , buďte opatrní.

Dávejte si pozor na podezřelé odkazy
Nikdy neklikejte na odkazy v e-mailech, které vypadají podezřele. Přihlašujte se vždy přes oficiální stránky UK.
Neprozrazujte svá hesla
Ani IT pracovníci po vás nikdy nebudou chtít heslo. Pokud o něj někdo žádá, jde o podvod.

Aktualizujte zařízení
Pravidelné aktualizace chrání váš počítač i mobil před útoky a viry.
Když si nejste jistí – neklikejte!
Raději si ověřte zprávu u IT podpory. Opatrnost se vždy vyplatí.