

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **107** ze dne **13.5.2025**

Jak poznat podezřelé přílohy a podvodné e-maily?

Jak fungují podvodné přílohy v e-mailech?

Podvodná příloha může vypadat jako běžný dokument – faktura, smlouva nebo třeba výpis z účtu. Když ji ale otevřete nebo kliknete na odkaz v takovém dokumentu, spustí se na pozadí škodlivý kód (malware). Ten pak může dělat různé věci: sledovat, co píšete na klávesnici (keylogger) , ukrást přihlašovací údaje, zašifrovat celý počítač (ransomware) nebo ho zapojit do sítě napadených zařízení (botnet)

V důsledku je cílem podvodného e-mailu nebo spamu vydělat peníze. Možností je řada, například vytěžit vaše data a prodat je, zapojit výpočetní výkon zařízení do těžby kryptoměn nebo třeba díky výpočetnímu výkonu umožnit provádět sofistikované útoky na korporace. V Česku nejčastěji podobné útoky těží data, zejména přihlašovací údaje. Útočníci s nimi pak obchodují na dark webu.

Pozor na zdvojené přípony

Útočníci často maskují podvodné přílohy pomocí tzv. zdvojené přípony. Například: V e-mailu vám odesílatel sděluje, že je nutné proplatit fakturu po splatnosti nebo dojde k zahájení exekuce. V příloze takového e-mailu je soubor faktura.pdf.exe. Na první pohled si člověk všimne jen ".pdf" a předpokládá, že jde o běžný dokument. Navíc, kdo by chtěl problémy s exekucí, že? Rychle jdete otevřít přílohu, abyste to vyřešili.

Ve skutečnosti je v příloze ale spustitelný program (.exe), který může po otevření nainstalovat škodlivý kód. Problém je, že některé e-mailové aplikace nebo Windows standardně nezobrazují celé přípony – takže uvidíte jen "faktura.pdf" a nepoznáte hned, že je něco špatně.

6 tipů, jak nebezpečnou přílohu poznat

Nejčastěji dostanete podvodný e-mail od neznámého odesílatele jako spam. Škodlivá příloha ale může přijít i od důvěryhodného zdroje, pokud útočníci napadli jeho e-mailový účet a zneužili k šíření malware.

1. E-mail jste neočekávali, ale píše se v něm o něčem důležitém. Útočníci pracují s našimi emocemi jako je strach (exekuce) nebo radost (náhodná výhra či dědictví). Podvodníci se často vydávají za autority (úřady, kurýry, IT podporu), aby vás přiměli přílohu otevřít.
2. Příloha má nezvyklou příponu. Soubory končící na .exe, .bat, .js, .vbs nebo .scr mohou být nebezpečné. Běžný dokument má většinou .pdf, .docx nebo .xlsx.
3. Případně má zdvojenou příponu, o tom, proč jsou zdvojené přípony nebezpečné se dočtete výše.
4. Příloha má příliš obecný název. Soubor pojmenovaný "dokument1.pdf" nebo "scan.zip" by měl vyvolat vaše podezření – útočníci často používají generické názvy.
5. Příloha obsahuje zazipovaný soubor. Soubory typu ZIP nebo RAR mohou skrývat škodlivý obsah. Někdy tento formát používají například finanční instituce pro zaslání smluv. Pokud ale danou zprávu neočekáváte, takový soubor neotevírejte.
6. Průvodní e-mail obsahuje překlepy a chyby. Útočníci často nejsou rodilí Češi, a proto jsou jejich e-maily v češtině strojově přeložené.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **107** ze dne **13.5.2025**

Na e-maily si dejte pozor v soukromí i v práci

Podvodné přílohy se objevují v osobních i v pracovních e-mailech. Útočníci dobře vědí, že v pracovním shonu lidé často otevírají přílohy bez velkého přemýšlení – hlavně když e-mail vypadá jako faktura, smlouva nebo interní žádost.

Právě na nepozornost a rutinu útočníci spoléhají. Stačí chvilka nepozornosti a nebezpečný soubor může spustit škodlivý kód nebo otevřít cestu do firemní sítě. Proto platí: raději se dvakrát zamyslet než jednou kliknout. Pokud si v pracovním prostředí nejste jistí, můžete se obrátit na IT oddělení.

Co dělat, když otevřete škodlivou přílohu?

- Pokud jste stáhli a otevřeli infikovanou přílohu, nepanikařte. V pracovním prostředí v první řadě upozorněte IT oddělení. Čím dříve se o problému dozvědí, tím lépe. Můžete tak doslova zachránit firmu před finančními ztrátami a technickými problémy.
- Nejprve odpojte zařízení od internetu. Tím zamezíte dalšímu šíření škodlivého kódu nebo odesílání dat. Rychle to provedete například přepnutím zařízení do režimu Letadlo.
- Změňte si důležitá hesla. Hlavně pokud jste v době otevření přílohy zadávali hesla (např. do banky, e-mailu). Zkontrolujte si bankovní účet, zda nedochází k nějakým neobvyklým transakcím.

Zdroj: AVcentrum ČR