

SPEAR-PHISHING

DOPORUČENÍ PRO PERSONÁL NEMOCNIC

- **Slepě neotevírejte přílohy a odkazy v e-mailech** – i zde platí okřídlené *“dvakrát měř, jednou řež”*
- **Kontrolujte e-mailovou adresu, ze které je e-mail odeslán** – hledejte chyby a překlepy, například `reditelstvi@fmmaletice.cz` místo `reditelstvi@fnmaletice.cz`
- **Zpozorněte, když obdržíte e-mail vytvářející časovou tíseň** – něco je třeba udělat *“hned teď”*
- **Zpozorněte, když obdržíte e-mail s neobvyklým požadavkem** – primář Vás žádá o okamžitý převod prostředků na účet zdravotnické firmy XY
- V případě nejistoty nebo podezření **kontaktujte vaše IT oddělení** – vzhledem k rizikům a finančním škodám, které může např. ransomware nemocnici způsobit, se na vás ani v případě planého poplachu nikdo na IT oddělení zlobit nebude.)
- **Omezte sdílení informací o zaměstnání na sociálních sítích** – nesdílejte detaily o své práci, pracovní procesy ani jména nadřízených, vše jde v rámci sociálního inženýrství zneužít k tomu, aby vás někdo nachytl
- **Nepovolujte makra v programech** - především v programech MS Office (Word, Excel...)

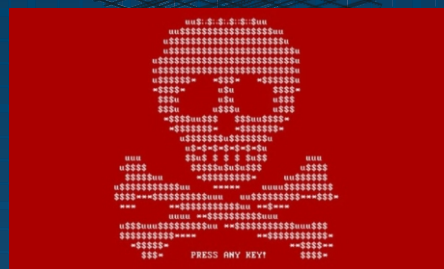
UPOZORNĚNÍ ZABEZPEČENÍ Bylo zakázáno spouštění makr. Povolit obsah



SPEAR-PHISHING ZBLÍZKA



Spear-phishing je nejčastěji podvodný e-mail usilující o to, aby uživatel stáhnul a spustil škodlivý software, nebo vyzradil své přihlašovací údaje. Tyto podvodné zprávy zpravidla imitují důvěryhodného odesílatele a cílí přímo na adresáta. Pro nemocnice a zdravotní zařízení se tak mohou vydávat i za zdravotnické organizace, jiné nemocnice nebo dodavatele zdravotnického materiálu. Mohou mít i formu SMS, telefonátu nebo zprávy na sociální síti.



Příklad ransomwaru Petya z roku 2016, který infikoval více než 300 000 počítačů.



83 % útočníků ve spear-phishingových e-mailech předstírají příslušnost ke známé značce (Microsoft, Apple, finanční instituce). Tím zvyšují svou legitimitu a obcházejí e-mailové filtry.



Cílem je instalace malwaru nebo krádež přihlašovacích údajů.



V e-mailu bývá odkaz na více či méně věrnou přihlašovací stránku služby, kterou útočníci napodobují



Poté, co uživatelé zadají své heslo, získají útočníci přístup k legitimnímu účtu uživatele, a mohou ukrást důvěrná data nebo účet využít k dalším útokům.

Od: Radek Chvalík <radek.chvallk@fmmaletice.cz>

Odesláno: 21. února 2020 9:44:19

Komu: Jaroslav.novak@fnmaletice.cz

Předmět: ověřit teď

Adresa je podvržená - končí @fmmaletice.cz

Vážený uživateli,

Zpráva vytváří časovou tíseň a vyzývá k rychlému jednání

Během včerejšího večera došlo k vypršení vašeho certifikátu na eReceipt. V návaznosti na to nebudete moci dále vydávat recepty. Pro jeho obnovení [klikněte zde](#) a urychleně zadejte své přihlašovací jméno a heslo.

<https://adminmicrosoftpda.wixisite.com/mysite>

Odkaz na závadnou adresu

Technická podpora

Fakultní nemocnice Maletice



Doporučení pro bezpečný pohyb v kybersvětě:

https://www.nukib.cz/download/vzdelavani/doporuceni/NUKIB_doporuceni_uzivatele_plakat.pdf



Další doporučení a vzdělávací kurzy:
<https://www.nukib.cz/cs/vzdelavani/>

www.nukib.cz

Národní úřad
pro kybernetickou
a informační bezpečnost

