VZDĚLÁVÁNÍ KYBERNETICKÉ BEZPEČNOSTI

Známou frázi o tom, že lidský faktor je nejslabším článkem v řetězu IT bezpečnosti jste jistě už slyšeli.
Ale školíte dostatečně své uživatele v oblasti IT bezpečnosti?
Často slýcháme, že na školení není čas, lidé, nebo nástroje skrze které by se důležité informace k uživatelům dostaly.

Ve VirusLabu se školení věnujeme naplno a protože víme, že každý zákazník má jiné potřeby i možnosti, nabízíme hned několik osvědčených způsobů vzdělávání.

Proškolte své zaměstnance dříve než bude pozdě.

VirusLab®

ŠKOLENÍ KYBERNETICKÉ BEZPEČNOSTI

Školení IT bezpečnosti prezenční formou je nejlepší variantou, kterou mohou Vaši zaměstnanci absolvovat. Jde o tři hodiny nabité informacemi, realizované pochopitelnou formou, srozumitelné pro skupiny až 50 uživatelů, doplněné množstvím praktických ukázek. Naše školení jsou pro posluchače nezapomenutelným zážitkem, po kterém změní nejen svá hesla, ale také návyky.
Kromě prezenčního školení je samozřejmě možné školení realizovat i formou webináře s možností pořízení záznamu, pokud by se někdo nemohl zúčastit v termínu.

- Zabezpečení hesel - jak na silná hesla, úniky a dvoufaktorové ověření
- E-maily a phishing - druhy, jak poznat podvody a jak se jim vyhnout
- Sociální inženýrství - metody, způsoby a obrana
- Sociální sítě – síla veřejně dostupných informací a jak jdou zneužít
- Bezpečné platby – jak a čím bezpečně platit a nenaletět
- Surfujeme internetem bezpečně – prohlížení webu má svá pravidla
- Bezpečnost mobilních zařízení – rizika přenosné kanceláře v kapse
- Fyzické zabezpečení – kamery, alarmy, drony a recepční

Školí Pavel Matějíček
etický hacker a konzultant kybernetické bezpečnosti

www.viruslab.cz +420 222 220 051 info@viruslab.cz

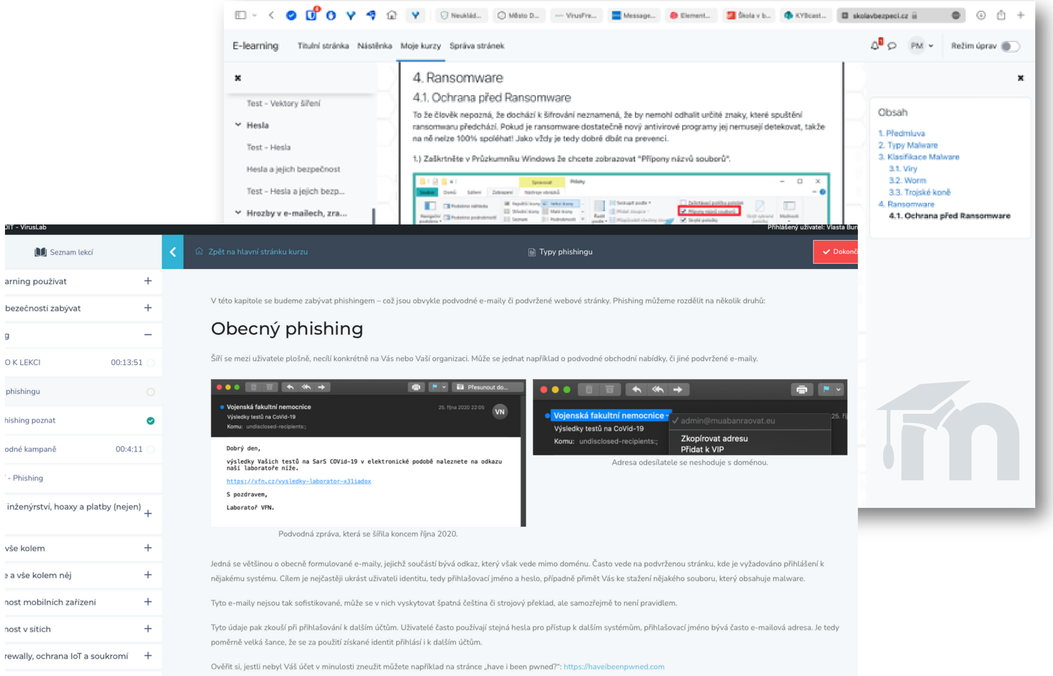
VirusLab®

E-LEARNING KYBERNETICKÉ BEZPEČNOSTI

Náš e-learning je rozdělený do 10 kapitol, které obsahují popis problematiky, instruktážní videa vč. ukázek konkrétních případů a test. Na konci kurzu pak absolvent získá certifikát o absolvování.
Poskytujeme i jako samotná data, připravená k implementaci do prostředí Moodle.

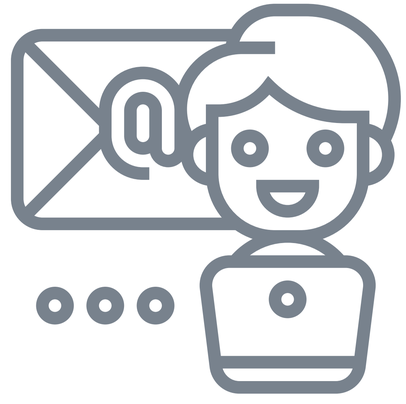
Témata kurzu:

- Jak e-learning používat
- Proč se bezpečností zabývat
- Phishing
- Sociální inženýrství, hoaxy a platby (nejen) on-line
- Hesla a vše kolem nich
- Malware a vše kolem něj
- Bezpečnost mobilních zařízení
- Bezpečnost v síťích
- Porty, firewally, ochrana IoT a soukromí
- Závěr



www.viruslab.cz +420 222 220 051 info@viruslab.cz

E-MAILOVÝ KURZ KYBERNETICKÉ BEZPEČNOSTI



Reikarnuje myšlenku korespondenční kurzů, je ekonomicky výhodný a nevyžaduje po zaměstnancích žádné větší úsilí. S e-mailem pracuje každý na denní bázi, nemusí se nikam přihlašovat, každý týden najde nový e-mail s novým tématem a videem ve schránce.

- 12 lekcí s tématy kybernetické bezpečnosti
- Lekce obvykle zasíláme 1x týdně
- Obsahem mailu je výstižný popis dané problematiky,
- konkrétní příklady z praxe pro lepší uchopení,
- krátké video s vysvětlením

- Závěrečný report jak lidé s emaily pracovaly a doporučení

Proč jste dostali tento e-mail

V dnešní době, kdy počet kybernetických útoků každým dnem roste, je potřeba se věnovat kybernetické bezpečnosti na mnoha úrovních a jednou z nich je i vzdělávání zaměstnanců.

Vektory šíření

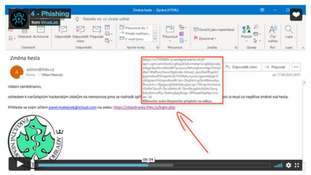
Než se ponoříme hlouběji do oblasti kybernetické bezpečnosti, pojďme se podívat na nejčastější a nejúčinnější techniky, které „ti zlí" používají, aby do vašeho počítače umístili svůj škodlivý kód nebo vás oklamali za účelem obohacení se.

Jak se k vám škodlivý kód dostane?

Statistika mluví jasně, více než 90 % škodlivého kódu se šíří prostřednictvím e-mailu. Důvod je ve skrze prostý, výroba hromadných kampaní je finančně nenákladná a dají se efektivně recyklovat. Samotným poštovním hrozbám, jakým je například phishing, se budeme věnovat v samostatném dílu.

Věříte cizím USB diskům?

Více o phishingu se dozvíte v tomto videu:



Přejít na video

Podvodné kampaně

Můžeme vám nabídnout sluneční brýle Ray-Ban s 90% slevou, nový iPhone nebo poukázku do Lidlu na víkendový nákup v hodnotě 1500 Kč? Vezmeme si za to jen údaje k vaší platební kartě a e-mailové schránce.

Říkáte si, že jsme se zbláznili? Jen si vzpomeňte, kolikrát jste v loňském roce zahlédli podobně "výhodné" nabídky například na Facebooku nebo vám odkaz poslal někdo z vašich známých.

Nechci slevu zadarmo

Stejně jako si dnes do bytu nepustíte podomní prodejce energií nebo vysavačů, který je mj. v mnoha městech zakázán, buďte i v online světě ostražití při výskytu podezřele výhodné nabídky. Některé e-shopy sice mají Black Friday několikrát ročně, nikdy však slevy nejsou astronomické. Zastavte se zamyslete se, na kolik taková nabídka může být legitimní.

Pár tipů, jak odhalit podvod

Jak si tedy vytvořit silné heslo?

To a mnohem více se dozvíte v tomto díle našeho IT kurzu.

Přejít na video

TOP 10 nejhorších hesel

1. 123456
2. Password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. letmein
8. 1234567
9. football
10. iloveyou

Bezpečné heslo pak vypadá třeba takto:

u*9@fexw6rrQQ!by

Toto heslo je dosti silné a jeho prolomení by trvalo několik let. Vidíte ten rozdíl proti nejhorším heslům zmíněným výše? Pro běžného uživatele je ale takové heslo bohužel nezapamatovatelné.

Bezpečnost on-line plateb

Začněme opět statistikou: jako Češi jme premianti v bezkontaktním placení, kdy každá devátá platba z deseti je bezkontaktní. Ruku v ruce s tím roste též obliba placení kartou na internetu, obzvláště tomu napomohl

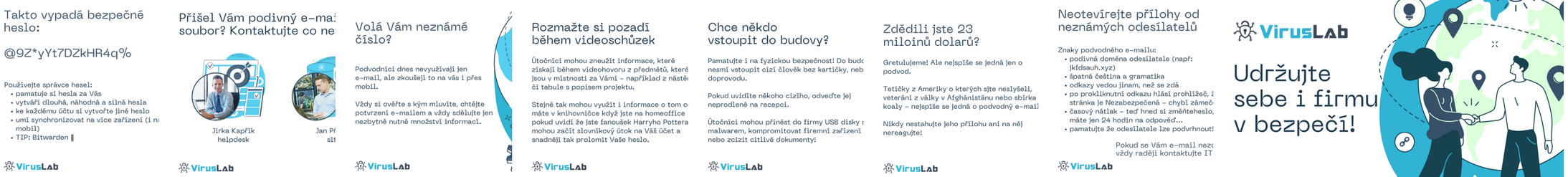
www.viruslab.cz
+420 222 220 051
info@viruslab.cz

SECURITY SCREEN-SAVER

Sada 25 obrázků s tématikou kybernetické bezpečnosti s možností mnohostranného použití. Obrázky jsou customizované ve Vašich firemních barvách a s vašimi kontakty.

- spořič obrazovky či zamykací obrazovka se mohou zdát nepodstatné, svojí funkčností však přispívají k zabezpečení vstupu do počítače. Navíc mohou sloužit k zobrazování užitečných informací jak před přihlášením, tak během doby, kdy je počítač uzamčen

- informační letáky jsou další cestou informační kampaně uživatelů. obrázky dodáváme v tiskové kvalitě a nic tak nebrání rozmístit je v prostoru aby byly více na očích



www.viruslab.cz +420 222 220 051 info@viruslab.cz