

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.



ŠKOLENÍ KYBERNETICKÉ BEZPEČNOSTI

Školení IT bezpečnosti prezenční formou je nejlepší variantou, kterou mohou Vaši zaměstnanci absolvovat. Jde o tři hodiny nabitě 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 nemoh 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



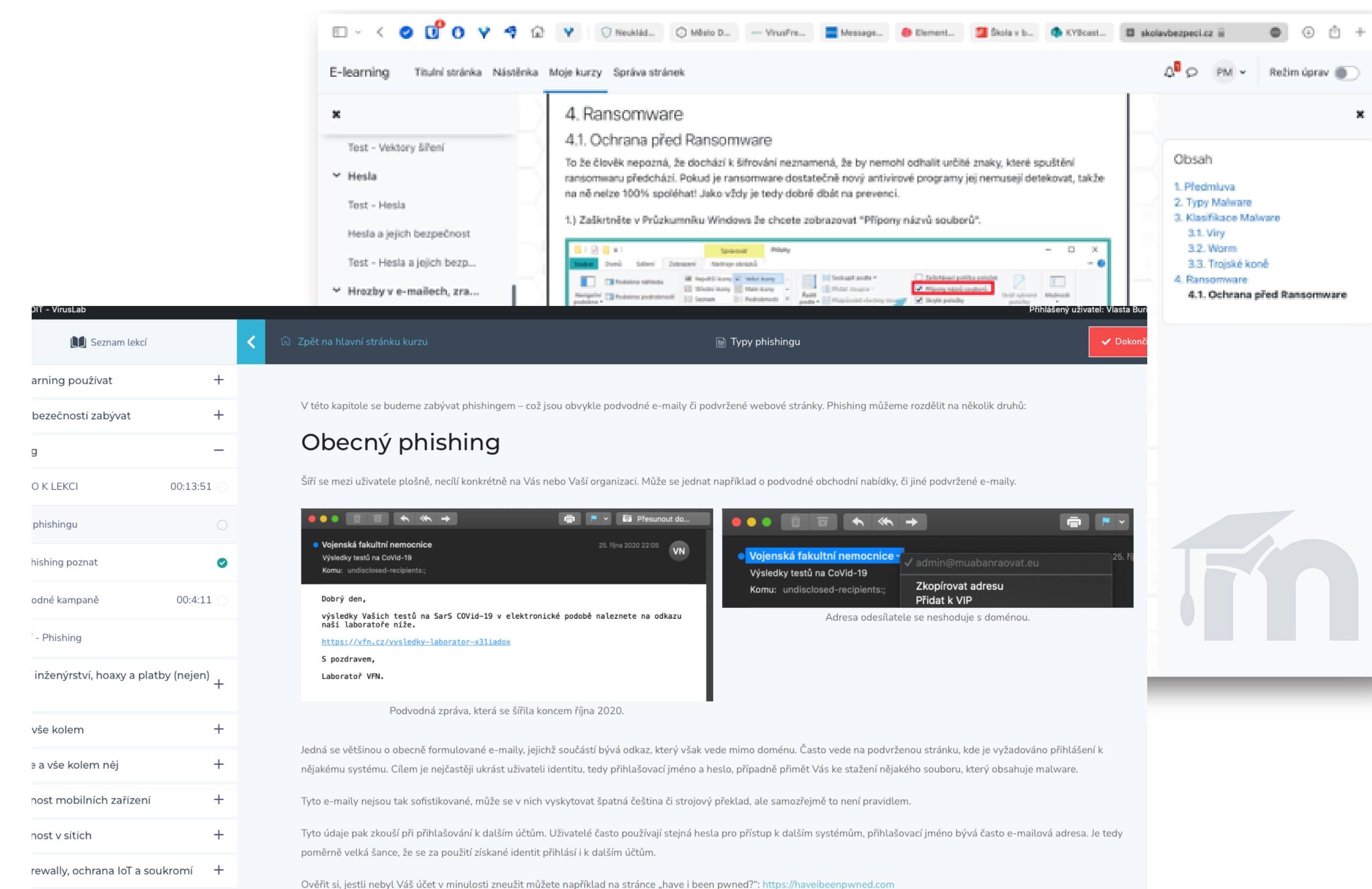
E-LEARNING KYBERNETICKÉ BEZPEČNOSTI

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 sítích
- Porty, firewally, ochrana IoT a soukromí
- Závěr



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



SECURITY SCREEN-SAVER

Sada 25 obrázků s tematikou 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

Takto vypadá bezpečné heslo:

@9Z*yYt7DZkHR4q%

Používejte správce hesel:

- pamatuje si hesla za Vás
- vytváří dlouhá, náhodná a silná hesla
- ke každému účtu si vytvoří jiné heslo
- umí synchronizovat na více zařízení (i na mobil)
- TIP: Bitwarden

 VirusLab

Přišel Vám podivný e-mail soubor? Kontaktujte co ne



Jirka Kapčík
helpdesk

 VirusLab

Volá Vám neznámé číslo?

Podvodníci dnes nevyužívají jen e-mail, ale zkoušejí to na vás i přes mobil.

Vždy si ověřte s kým mluvíte, chtějte potvrzení e-mailem a vždy sdělte jen nezbytně nutné množství informací.

 VirusLab

Rozmažte si pozadí během videoschůzek

Útočníci mohou zneužít informace, které získají během videohovoru z předmětů, které jsou v místnosti za Vámi – například z nástěny či tabule s popisem projektu.

Stejně tak mohou využít i informace o tom co máte v knihovničce když jste na homeoffice – pokud uvidí že jste fanoušek Harryho Pottera mohou začít slovníkový útok na Váš účet a snadněji tak prolomit Vaše heslo.

 VirusLab

Chce někdo vstoupit do budovy?

Pamatujte i na fyzickou bezpečnost! Do budovy nesmí vstoupit cizí člověk bez kartičky, neb doprovodu.

Pokud uvidíte někoho cizího, odvedte jej neprodleně na recepci.

Útočníci mohou přinést do firmy USB disky s malwarem, kompromitovat firemní zařízení nebo zcizit citlivé dokumenty!

 VirusLab

Zdědili jste 23 milioňů dolarů?

Gretulujeme! Ale nejspíše se jedná jen o podvod.

Tetičky z Ameriky o kterých jste neslyšeli, veteráni z války v Afghánistánu nebo sbírka koaly – nejspíše se jedná o podvodný e-mail

Nikdy nestahujte jeho přílohu ani na něj nereagujte!

 VirusLab

Neotevírejte přílohy od neznámých odesílatelů

Znaky podvodného e-mailu:

- podivná doména odesílatele (např: jkfdsauh.xyz)
- špatná čeština a gramatika
- odkazy vedou jinam, než se zdá
- po prokliknutí odkazu hlásí prohlížeč, že stránka je Nebezpečná – chybí zámeček
- časový nátlak – teď hned si změňte heslo, máte jen 24 hodin na odpověď...
- pamatujte že odesílatele lze podvrhnout!

Pokud se Vám e-mail nezvedá raději kontaktujte IT

 VirusLab

 VirusLab

Udržujte sebe i firmu v bezpečí!

