

# 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 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 zúčastnit 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



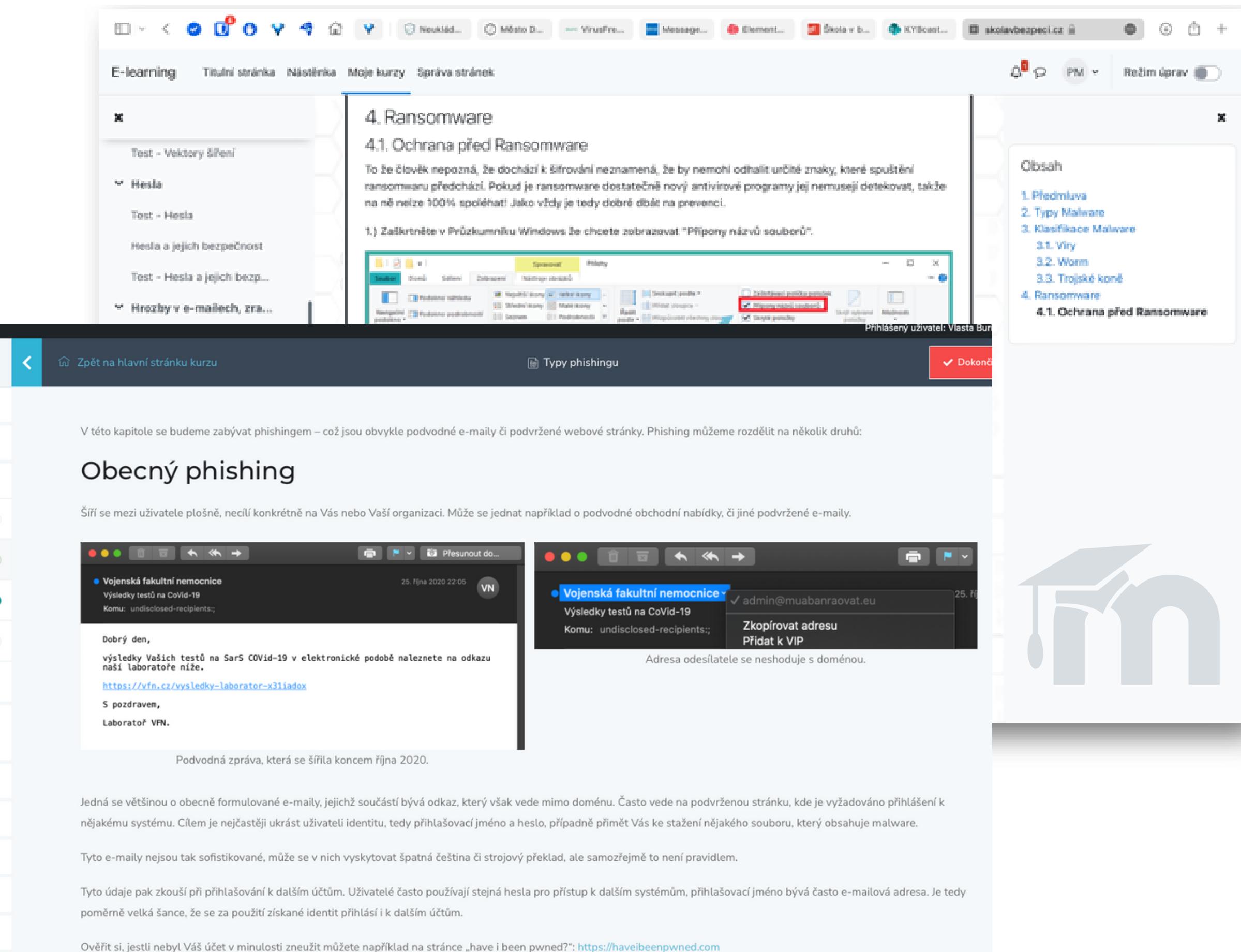
# E-LEARNING KYBERNETICKÉ BEZPEČNOSTI

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

The screenshot shows a Moodle-based e-learning interface. On the left, there's a sidebar with course navigation and a search bar. The main content area displays a chapter titled "4. Ransomware" with a sub-section "4.1. Ochrana před Ransomware". It includes text about ransomware, screenshots of Windows File Explorer showing encrypted files, and two examples of phishing emails from "Vojenská fakultní nemocnice" asking for COVID-19 test results. The right side of the screen shows a large watermark of a graduation cap and a person icon.

# 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

The image shows a woman with dark hair and glasses, wearing a white sleeveless top, standing in a server room. She is holding a tablet computer and looking at it. The background is filled with rows of server racks, their lights glowing in a blur of blue and green. The overall atmosphere is one of a high-tech, data-centric environment.

## 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 ponoríme 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?

**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 zahledli 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 vysavačů, který je mj. v mnoha městech zakázán, budete i v online ostražití při výskytu podezřele výhodné nabídky. Některé e-shopy sice Black Friday několikrát ročně, nikdy však slevy nejsou astronomické. Zase se zamyslete se, na kolik taková nabídka může být legitimní.

**Pár tipů, jak odhalit podvod**

# Jak si tedy vytvořit silné heslo

## 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<sup>\*</sup>9@fexw6rrQQ!by**

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

The image shows a woman with glasses and a white top, standing in a server room filled with racks of server hardware. She is looking at a tablet device. A large, semi-transparent digital interface is overlaid on the scene, featuring various data visualizations such as bar charts, line graphs, and network diagrams in shades of blue and green. This interface represents the 'Bezpečnost on-line plateb' (Online payment security) mentioned in the text below.

## 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



Takto vypadá bezpečné heslo:

@9Z\*yYt7DZkHR4q%

Používejte správce hesel:  
 • pamatuje si hesla za Vás  
 • vytváří dlouhá, národní a silná hesla  
 • každému účtu si vytvořte jiné heslo  
 • umí synchronizovat na více zařízení (i na mobil)  
 • TIP: Bitwarden !!



Přišel Vám podivný e-mail soubor? Kontaktujte co ne-





Volá Vám neznámé číslo?





Rozmažte si pozadí během videoschůzek

Útočníci mohou zneužít informace, které žáskají během videohovoru z předmětu, které jsou v místnosti za Vámi – například z nástění či tabule s popisem projektu.

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



Chce někdo vstoupit do budovy?

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

Pokud uvidíte někoho cizího, odvedte jej neprodleně na recepci.

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



Zdědili jste 23 milionů dolarů?

Gretulejeme! Ale nejspíše se jedná jen o podvod.

Tetišky z Ameriky o kterých slyšeli, veterán z války v Afghánistánu nebo sbírka koaly – nejspíše se jedná o podvodný e-mail.

Nikdy nestahujte jeho přílohu ani na něj nereagujte!



Neotevírejte přílohy od neznámých odesílatele

Znaky podvodného e-mailu:

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

Pokud se Vám e-mail nezvídavý raději kontaktujte IT





Udržujte sebe i firmu v bezpečí!

