IMPULS
PRO KARIÉRU
A PRAXI

2023

KYBERNETICKÁ BEZPEČNOST PRO SŠ

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Jhk.cz

JIHOČESKÁ HOSPODÁŘSKÁ KOMORA

Jihočeský kraj

Pracovní postup „Kybernetická bezpečnost pro SŠ“ je součástí publikace „Pracovní postupy pro workshopy digitalizace ve školách.“, která vznikla v rámci aktivity Asistenčního centra Impuls pro kariéru a praxi při Jihočeské hospodářské komoře díky realizaci projektu „Implementace Krajského akčního plánu Jihočeského kraje III“, který je spolufinancován Evropskou unií. Registrační číslo projektu CZ.02. 3. 68/0.0/0.0/19_078/0018246

Elektronická verze publikace je k dispozici na **www.impulsprokarieru.cz**

Autoři:
Ing, Rudolf Vohnout, Ph.D., Přírodovědecká fakulta, Jihočeská univerzita,
Ing. Petr Břehovský, Přírodovědecká fakulta, Jihočeská univerzita
Editor: doc. RNDr. Ing. Jana Kalová, Ph.D.
Publikaci připravila Přírodovědecká fakulta Jihočeské univerzity

Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta
Centrum pro přírodovědné vzdělávání

Grafický design: Čestmír Sukdol – www.brandi.cz

Vydala: Jihočeská hospodářská komora

2021

Obsah

Cílem workshopu je na praktických příkladech demonstrovat důsledky nezodpovědného chování v online prostoru. Workshop bude v první, teoretické části cílen na osvětu návyků chování na internetu a to primárně v oblasti včasné detekce závadného obsahu. V části praktické pak bude konkretizováno, jakým způsobem lze závadný obsah identifikovat a jaká jsou pravidla pro práci s ním. V závěrečné části budou rozebrány důsledky nevěnování dostatečné obezřetnosti chování na internetu.

Základní instrukce

Tento kurz je doporučován pro studenty středních škol a vyšší ročníky víceletých gymnázií. Pokud je na ZŠ vyučována informatika intenzivně (např. již od 3. třídy), může být kurz doporučen také pro vyšší ročníky (8.+9. třída) druhého stupně ZŠ. Předpokládá se ne úplně základní orientace v online světě a běžné využívání chytrých zařízení připojených bez kontroly k internetu (smartphone, tablet, notebook apod.) Kurz je koncipován jako pokročilá problematika uvědomělého chování v online prostředí, kde bohužel díky množství informací se obezřetnost a bezpečnost dostává na druhou kolej.

Časová dotace tohoto kurzu je stanovena na 6 hodin. Rozdělení 4+2 hodiny na teoretický a legislativní základ a získání praktických dovedností v oblasti detekce podvodného obsahu. Učitel by měl nejprve prostudovat všechny materiály dané k tomuto kurzu a pak se sám rozhodnout, kolik času kurzu věnovat.

Doporučený průběh a časové dotace podrobněji. Kurz lze rozčlenit do následujících částí:

1. Teoretický a legislativní úvod – především vymezení mantinelů a pojmu kybernetická bezpečnost, zákon o kybernetické bezpečnosti a kyberkriminalita. S tím spojená identita na internetu a taktiky vylákání informací.
   a. Doporučuji dvě vyučovací hodiny.
2. Praktické ukázky podvodných elektronických zpráv a proč na internetu platí více než kde jinde rčení „dvakrát měř, jednou řež“. Na konkrétních příkladech ukážeme, jak lze podvody identifikovat a to včetně jejich analýzy a diskuse.
   a. Doporučuji dvě vyučovací hodiny.
3. Plnění zadaných úkolů dle již předzpracovaných kvízů či online testů. Případně dle pracovních listů vypracovaných vyučujícím.
   a. Pro každý list či kvíz doporučuji jednu vyučovací hodinu.

Pro co největší dopad praktické části je více než vhodné zjistit, jací studenti budou v rámci výuky tohoto tématu vzdělávání a kolik veřejně dostupných informací lze o jednotlivých osobách dohledat. Pro zaslání testovacích phishingových útoků je nutné znát funkční emailové adresy studentů.

Teoretická část k dané problematice

Kybernetická bezpečnost

> *Kybernetická bezpečnost nemá ucelenou definici. Zásadní je si uvědomit, že vždy představuje nějaký soubor opatření vedoucí k ochraně před kriminálním či neautorizovaným užitím elektronických dat. Jinými slovy přijmutí takových opatření, která vedou k dosažení tohoto stavu. Tato opatření mohou být jak bezpečnostní, tak technické či organizační (administrativní) povahy.*
>
> *Souhrn právních, organizačních, technických a vzdělávacích prostředků, které směřují k zajištění* ***ochrany*** *počítačových systémů a dalších prvků ICT, aplikací,* ***dat a uživatelů***
>
> **+**
>
> *schopnost počítačových systémů a využívaných služeb reagovat na kybernetické hrozby či útoky a jejich následky, jakož i plánování obnovy funkčnosti počítačových systémů a služeb s nimi spojených.*

Dále je důležité se seznámit s kybernetickou hrozbou. Jedná se o možnost škodlivého pokusu o narušení počítačové sítě nebo systému. Kybernetickou hrozbu lze také definovat jako akt směřující ke změně informace, aplikací či systému samotného. Kybernetická hrozba může způsobit:

- Únik informace – stav, kdy dojde k vyzrazení chráněné informace neautorizovanému subjektu.
- Narušení integrity – poškození, změna, či vymazání dat.
- Potlačení služby – úmyslné bránění v přístupu k informacím, aplikacím, či systému.
- Nelegitimní použití – užití informací neautorizovaným subjektem či neoprávněným způsobem.

„Ten, kdo se ve jménu bezpečnosti vzdává svobody, nezaslouží si ani svobodu, ani bezpečnost.“

Benjamin Franklin

Kybernetická hrozba a kriminalita

Kolouch a spol. (2018) kybernetickou hrozbu definuje jako akt směřující ke změně informace, aplikací či systému samotného.

Kyberkriminalitu lze definovat jako jednání namířené proti počítačovému systému, počítačové síti, **datům či uživatelům** nebo jako jednání, při němž je počítačový systém použit jako nástroj pro spáchání trestného činu.

V tomto kurzu se budeme výhradně soustředit na **Phishing**, resp. **Spearing**. Jedná se o podskupinu tzv. **Sociálního inženýrství**. To představuje techniky pro manipulování osob, což není nic jiného než vhodné aplikování psychologických metod. Typickými příznaky nátlaku jsou

- Vydávání se za autoritu – (kyber)kriminálník se snaží vzbudit dojem, že s Vámi hovoří z nadřízené pozice v projednávané záležitosti (nadřízený, policista, exekutor apod.).
- Hrozba ztráty (příležitosti) – je důvod, který Vás má přimět jednat, abyste neutrpěli ztrátu (neodtáhli Vám automobil, nezavřeli Vás do vězení apod.) nebo abyste nepřišli o příležitost si přilepšit (nevyhrajete dovolenou na Bahamách, nepovýší Vás apod).
- Časová tíseň – (kyber)kriminálník Vás nesmí nechat přemýšlet, abyste ho neodhalili, proto Vás bude nutit reagovat rychle, pudově (do hodiny Vám zablokujeme účet, hned zítra Vás vyhodí z práce apod.).
- Utajování – (kyber)kriminálník si je vědom, že i když Vás zmanipuloval, můžete se o jeho požadavku zmínit kolegovi, který není zmanipulován a může tedy podvod snadněji prohlédnout. Často se Vás bude snažit přesvědčit, že utajování je pro Vás výhodné (nechcete, aby Vám kolegové záviděli, jde o citlivé informace, jde o státní zájem apod.)

Pokud se v jakékoliv komunikaci setkáte s výše uvedenými příznaky, velmi pravděpodobně se Vás někdo snaží podvést.

- Zdroj hrozby *způsobený člověkem*.
- Formu zavinění: *úmyslná*.

Motivace takového činu lze rozdělit:

- Za účelem získání finančního prospěchu.
- Za účelem získání konkurenční převahy.
- Za účelem dokázání svých schopností.
- Za účelem odplaty.
- Z důvodu neplnění povinností.

Základní legislativa

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
  - vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
- Zákon č. 110/2019 Sb. Zákon o zpracování osobních údajů (aka GDPR)
- Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

Doménový základ

Doručené zprávy často obsahují odkazy na webové stránky a před jejich návštěvou je dobré si rychlým pohledem zkontrolovat, zda nejsou podezřelé. Na příkladovém odkazu (URL) si nejprve ukážeme důležité části každého odkazu.

https://connect.jcu.cz/pokus/?launcher=false

https:// – definuje, jakým protokolem se stránkou náš prohlížeč komunikuje

connect.jcu.cz – doménové jméno serveru, tj. kam se připojujeme

/pokus/ – detailnější specifikace toho, co od serveru chceme získat

?launcher=false – parametry, kterými upřesňujeme, co od serveru chceme

*Kdybychom měli výše uvedené URL převést do srozumitelné věty, zněla by asi takto: Prohlížeči můj webový, prosím tě, zajdi na **web connect.jcu.cz** a dones mi data z lokality pokus , a když se budou ptát jestli chci launcher, řekni jim, že ne. Jo a ten server umí nářečí https, tak se přepni do této řeči.*

Doménové jméno je identifikátor, který se skládá z jednotlivých částí (tzv. label) oddělených tečkami. Čím více je label *vpravo*, tím je *obecnější* → geograficky si to lze představit například jako umístění ulice ve městě, státě, kontinentu, planetě. Také záleží na pořadí.

branisovska.cb.cz.europe.earth.space

Každá změna v doménovém jméně znamená, že jde o úplně jiný identifikátor, například

branisovska.plzen.cz.europe.earth.space – ulice je v jiném městě

branisovska.cb.de.europe.earth.space – ulice je v jiném státě

branisovska.cb.cz.usa.venus.space – ulice je na jiném kontinentu

branisovska.cb.cz.europe.venus.space – ulice je na jiné planetě

cb.branisovska.cz.europe.earth.space – jde o ulici CB ve městě branisovska

Co je a jak rozeznat phishing

Volně jej lze definovat jako činnost, při které se útočník záměrně snaží vylákat osobní údaje (většinou přístupové, či finanční) za účelem jejich zneužití. Toho dosahuje buď vydáváním se za někoho jiného (píše ti tvůj učitel, že máš pětku) či zneužitím důvěřivosti předstíráním organizace (píše ti tvá škola, že máš ředitelskou důtku). V drtivé většině se jako medium používá elektronická pošta (email).

Jinými slovy se jedná o sociální inženýrství aplikované do zpráv elektronické pošty s cílem získat přihlašovací údaje (jméno a heslo) se označuje pojmem phishing.

Existují také specializované formy Phishingu:

- **Spearing** (či spear phishing) – je sofistikovaný útok využívající interní informace o službách, lidech či majetku dané organizace k provedení cíleného phishingového útoku. Bude podrobně rozebrán v příkladech z praxe.
- **Pharming** – technicky pokročilý útok manipulací s DNS serverem, kdy útočník získá kontrolu nad překlady doménových jmen na IP adresy. Přesměrování probíhá na servery kontrolované útočníkem.

Emailová adresa
Překontrolujte doménu a jméno. Generické adresy jsou podezřelé.

Hlavička
Kompletní hlavička emailu popisuje, přes jaké servery byl email doručován. Neobvyklé servery mohou znamenat phishing.

Oslovení
Jak Vás obvykle odesílatel oslovuje? Liší se nějak oslovení od obvyklého?

Rozloučení
Neliší se rozloučení od obvyklého?

Odkazy
Postavte myš na odkaz aniž byste klikali a podívejte se, zda není podezřelý.

Přílohy
Přílohy od podezřelých odesílatelů jsou většinou škodlivé.

Forma
Je dopis správně česky?
Snaží se Vás pisatel dostat do časové tísně?
Příliš dobré, nebo naopak příliš špatné zprávy.

Čas odeslání
Útočníci často pracují v jiném časovém pásmu. Pokud je tedy čas odeslání v hlubokých nočních hodinách, může to být podezřelé.

Kyberkriminálníci (až na velmi vzácné případy) nemůžou použít doménové jméno serveru, za který se vydávají, takže volí obvykle některou z následujících strategií.

1. případ:
Vůbec se nesnaží skrývat a doufají, že na URL se nikdo nedívá; pak se lze setkat například s takovýmito adresami:
http://1.1.1.2/login.php – použití IP adresy v odkazu
https://super.domain.eu?login=ap@jcu.cz – zcela náhodná doména

2. případ:
Předpokládají, že uživatel neví, jak se správná doména jmenuje, a zkusí něco, co vypadá podobně:
https://jcu.eprihlaseni.cz/login – jiné pořadí jednotlivých částí domény

3. případ:
Pozornější uživatele zkusí ošálit použitím textu, který odpovídá doménovému jménu, v jiné části URL:
http://shortdomain.cz/login.jcu.cz – doména je ve specifikaci cesty
http://www.ucj.cz?param=login.jcu.cz – doména je v parametru

4. případ:
Použijí doménové jméno, které je podobné, a doufají, že to uživatel přehlédne:
https://login.jcuu.cz – doména se velmi podobá
https://login-jcu.cz – vložená pomlčka zcela mění význam
https://login.jcu.cc – změna v jednom písmenu

Pokud už stránku navštívíme, může nám pomoci také skutečnost, zda stránka používá zabezpečené spojení (https). Zde je třeba provést kontrolu certifikátu. Pokud se jedná o „Let's Encrypt" je třeba se mít na pozoru.

Existují také specializované iniciativy, které se problematikou phishingu zabývají. Neznámější je asi „Anti Phishing Working Group"

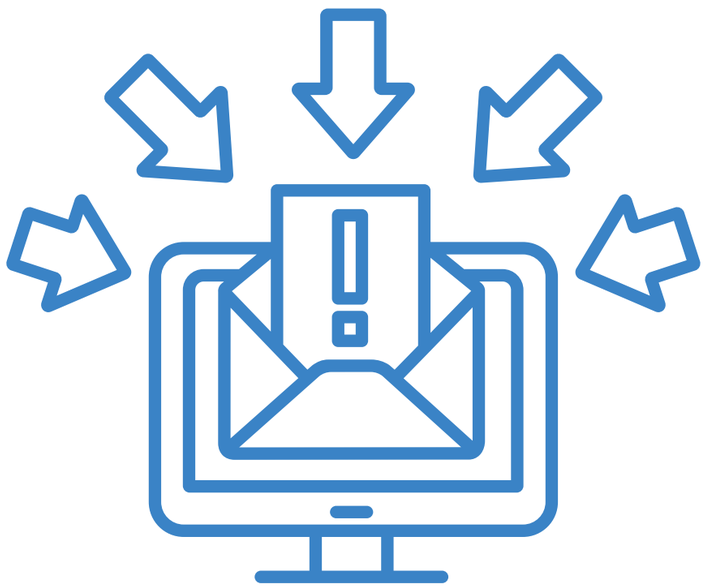
https://apwg.org/about-us/

Doporučené odkazy a materiály pro hlubší porozumění problematiky

[1] **https://www.eset.com/cz/blog/prevence/phishing-stoji-za-tretinou-pruniku-jak-poznat-skodlive-e-maily/**

[2] **https://edu.ceskatelevize.cz/video/119-phishing**

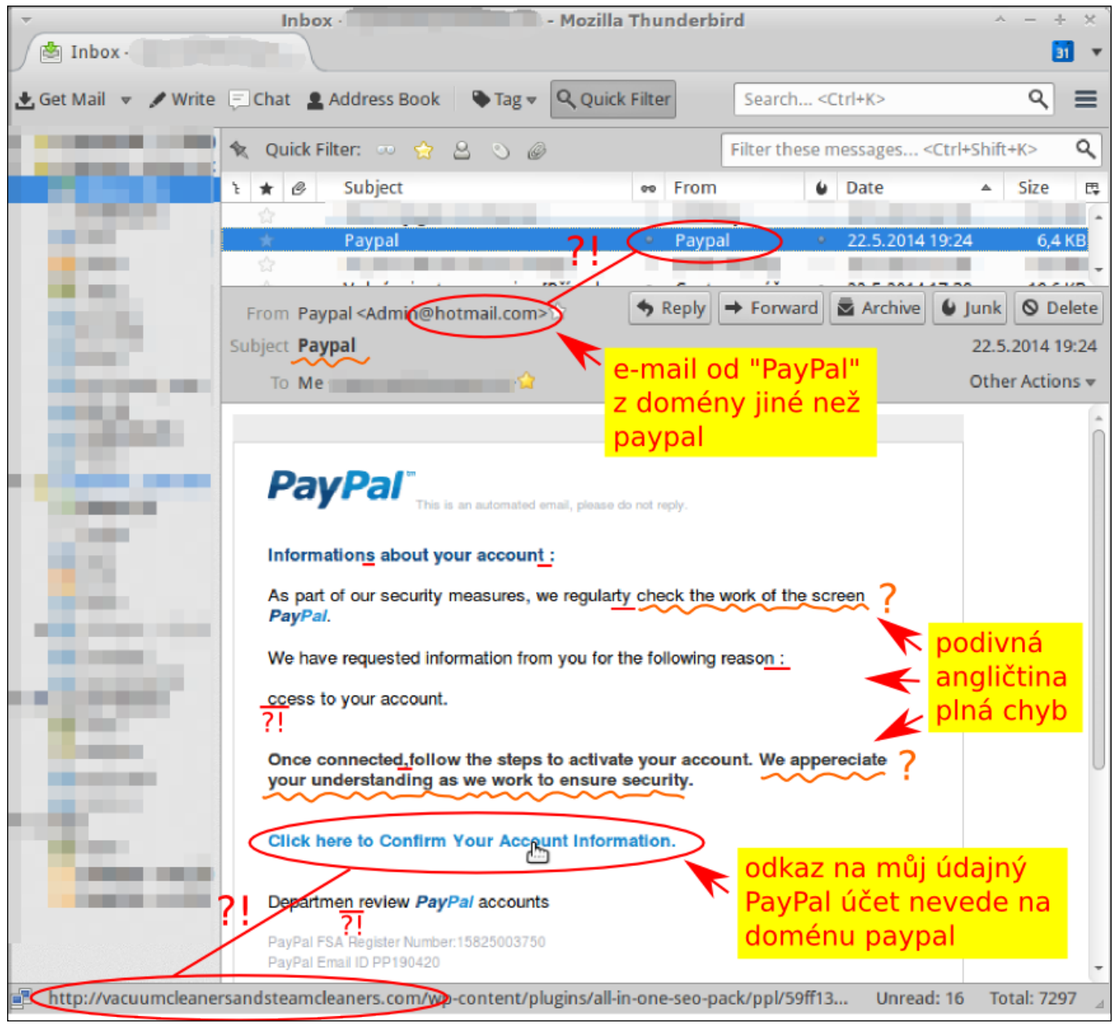
[3] **https://kyberbezpecnost.csirt.cz/cs/kyberbezpecnost/pro-uzivatele/phishing-jak-jej-vcas-rozpoznat-a-nenaletet/**



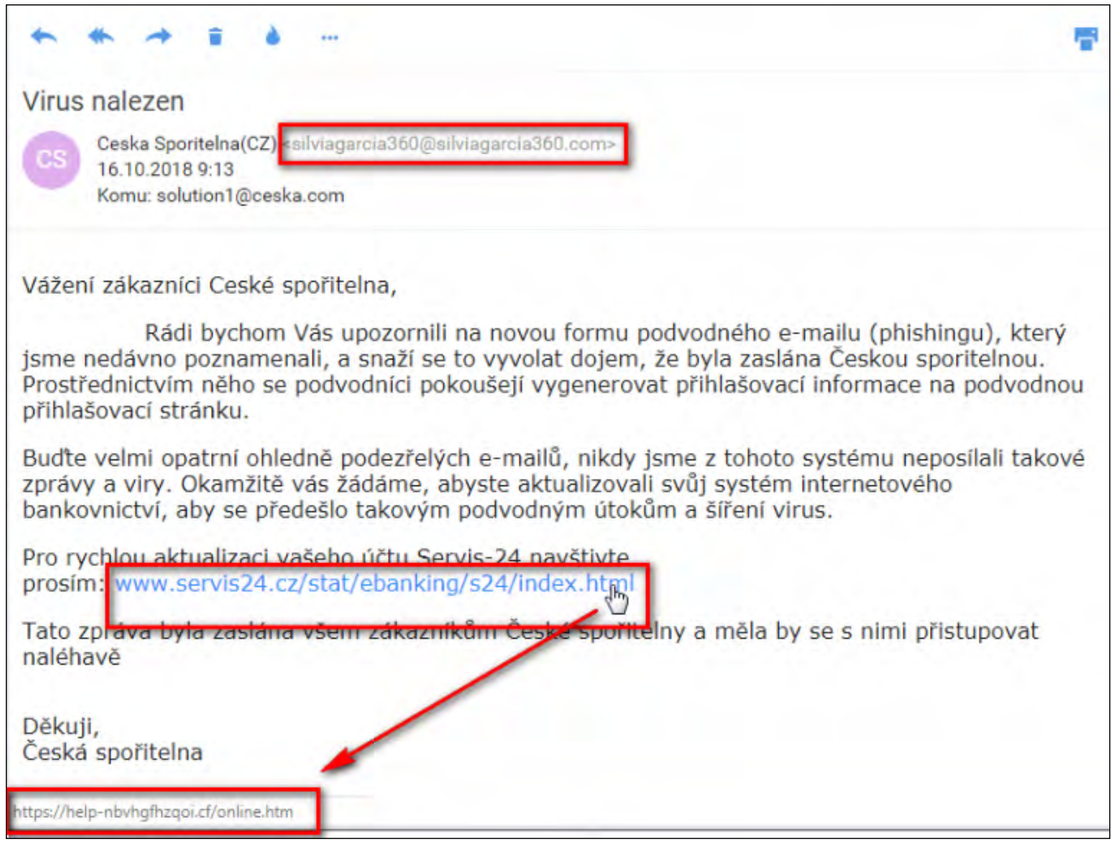
Příklady z praxe

Níže uvádíme konkrétní příklady z praxe podvržených emailů včetně podrobného rozboru, jak je lze identifikovat.

Jak si můžete povšimnout, nejzásadnějším vodítkem je odkaz na nevalidní doménu. U těch více amatérských je také adresa odeslání, ta, které nepatří doména dané instituce (níže tedy Paypal a Česká spořitelna).



Obrázek 1: Paypal Phishing

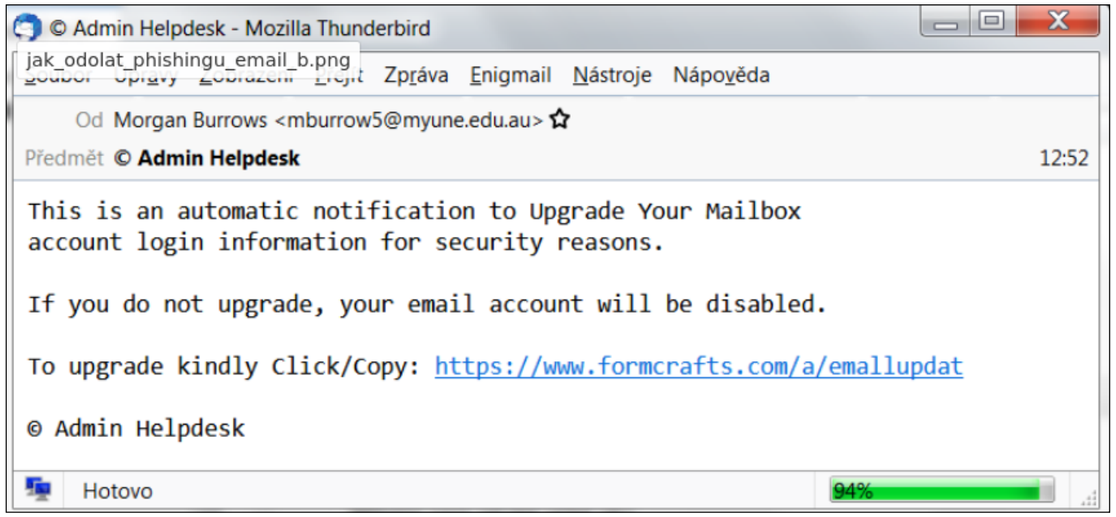


Obrázek 2: Česká spořitelna Phishing

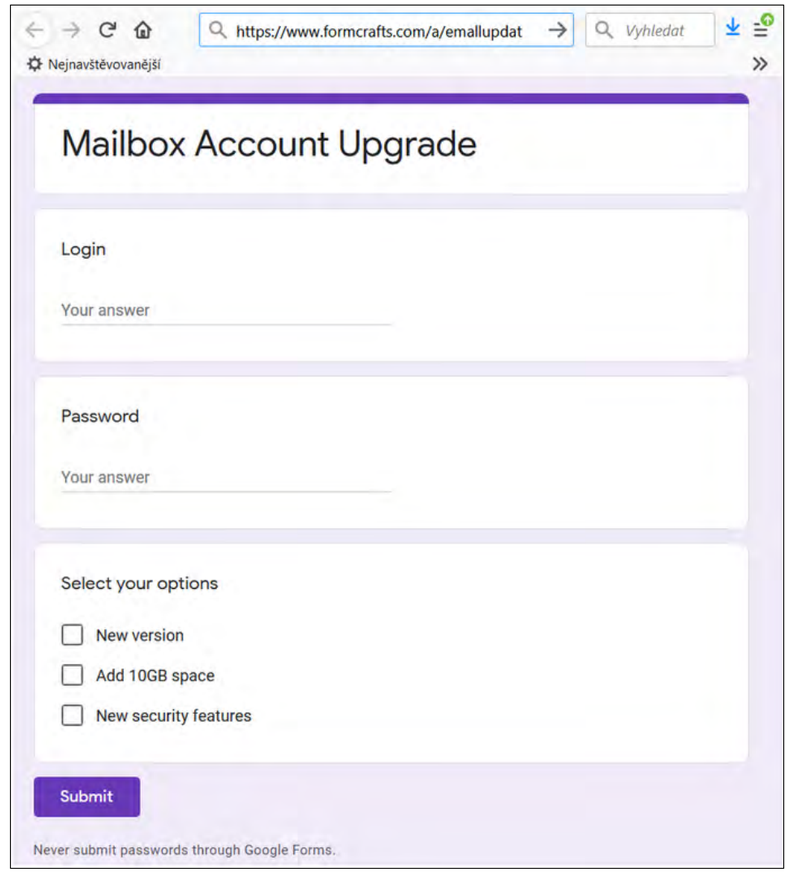
Podvodné zprávy se závadnou přílohou (typicky malware) již nejsou tak časté. V drtivé většině případů je totiž odhalí poštovní brány a antivirová řešení.

Co ovšem časté je, jsou typicky odkazy na formuláře, které vypadají jako skutečné (typicky Google nebo Microsoft Forms) a jen tak mimoděk po Vás také chtějí jméno a heslo.

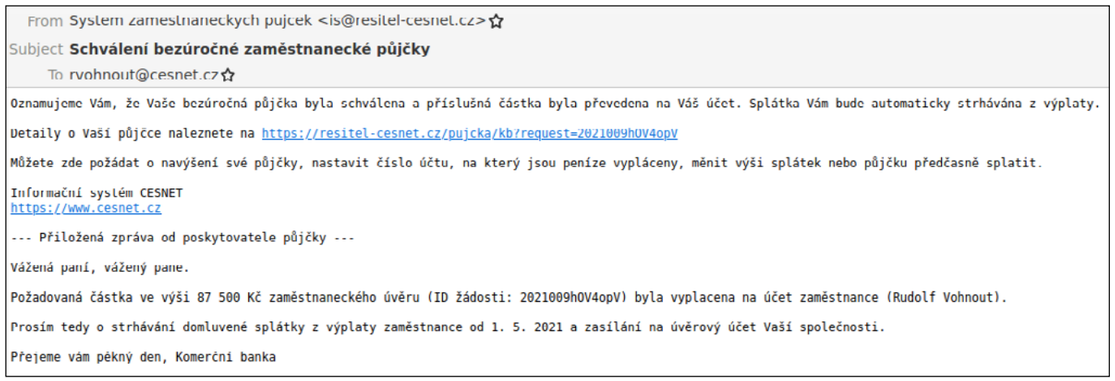
Začíná být stále více běžnou praxí, že si firmy (ale také školy) testují interně své zaměstnance za účelem zjištění jejich schopnost identifikovat podvržené emailové zprávy. Tomuto kroku ale většinou předchází (většinou povinně) školení. Jeho absolvování bývá stvrzeno podpisem. Ne vždy ovšem takové školení přinese kýžený efekt (zaměstnanci neposlouchají, nudí se apod.). Proto se potom přistupuje právě k testování v reálném prostředí.



Obrázek 3: Google Forms Phishing



Níže je uveden jeden takový příklad. Pod ním bude rozebráno, jak lze identifikovat, že se jedná o podvrženou zprávu.


From Systém zaměstnaneckých půjček <is@resitel-cesnet.cz>
Subject **Schválení bezúročné zaměstnanecké půjčky**
To rvohnout@cesnet.cz

Oznamujeme Vám, že Vaše bezúročná půjčka byla schválena a příslušná částka byla převedena na Váš účet. Splátka Vám bude automaticky strhávána z výplaty.

Detaily o Vaší půjčce naleznete na https://resitel-cesnet.cz/pujcka/kb?request=Z021009hOV4opV

Můžete zde požádat o navýšení své půjčky, nastavit číslo účtu, na který jsou peníze vypláceny, měnit výši splátek nebo půjčku předčasně splatit.

Informační systém CESNET
https://www.cesnet.cz

--- Přiložená zpráva od poskytovatele půjčky ---

Vážená paní, vážený pane.

Požadovaná částka ve výši 87 500 Kč zaměstnaneckého úvěru (ID žádosti: 2021009hOV4opV) byla vyplacena na účet zaměstnance (Rudolf Vohnout).

Prosím tedy o strhávání domluvené splátky z výplaty zaměstnance od 1. 5. 2021 a zasílání na úvěrový účet Vaší společnosti.

Přejeme vám pěkný den, Komerční banka

Obrázek 4: CESNET Spearing

Obrázek 3 představuje už celkem sofistikovaný spearing. Ve společnosti CESNET totiž:

- Mají systém bezúročných zaměstnaneckých půjček.
- Existuje důležitý interní systém Řešitel.
- Komerční banka je hlavní bankou společnosti.

Bližší analýza:

- Text neobsahuje žádné pravopisné chyby ani překlepy.
- Doména „resitel-cesnet.cz“ skutečně existovala – je však založena pouze za účelem tohoto spearingového útoku. Předpokládá se, že každý uživatel internetu ví, že jednotlivé úrovně domén se odlišují tečkami.
- O žádnou půjčku jste nežádal.

Účelem je ze zaměstnanců vylákat jejich přístupové údaje (i když v tom případě pouze pro testovací účely) – pokud je zaměstnanec zadá správně, zobrazí se mu stránka s informací, že se stal obětí podvodné emailové zprávy, ale naštěstí pouze testovací a nemusí se tak obávat následků.

U phishingu a spearingu je vždy nutné věnovat analýze takových zpráv čas, pokud se Vám něco na první pohled nepozdává.

Relevantní odkazy

[1] **https://support.zcu.cz/index.php/Phishing_-_p%C5%99%C3%ADklady**

Pro ty, co si chtějí rozšířit obzory:

https://knihy.nic.cz/files/edice/cybersecurity.pdf

https://support.zcu.cz/index.php/Phishing

https://www.csfd.cz/film/812238-socialni-dilema/

https://www.documentaryarea.tv/player.php?title=The%20Social%20Dilemma

Metodická a didaktická část

Na úvod je vhodné uvést, že pro tento kurz nejsou připravovány žádné pracovní listy. Je totiž žádoucí, aby si je připravil sám vyučující na základě mnoha odkazů v tomto materiálu. Dále je mnohem flexibilnější, pokud studenti obdrží pracovní listy v elektronické podobě ve formátu PDF než vytištěné. Přepisováním případných odkazů do internetového prohlížeče může dojít k překlepům a tudíž zbytečnému zdržování.

Phishingové a kyberbezpečnostní testy

1) Nejedná se přímo o pracovní listy, ale berte tuto sekci jako námět k jejich vytvoření. Zkuste, ať si studenti zkusí udělat online test zdali dokáží podvodné zprávy sami rozpoznat. Poté konzultujte s nimi jejich úspěšnost a nechte je v případě neúspěchu mezi sebou probírat jednotlivé příklady.
[1] **https://phishingquiz.withgoogle.com/**
[2] **https://www.sonicwall.com/phishing-iq-test/**

2) Jako ještě sofistikovanější doporučujeme perzonalizovaný phishingový test z
https://phishing-iq-test.com/

3) Pro pokročilé procvičení kybernetické bezpečnosti velmi doporučujeme absolvovat a do pracovních listů zahrnout komplexní online test, který podporuje Česká bankovní asociace a Policice České republiky.
https://kybertest.cz/

*Velmi doporučujeme zařadit do výuky (a také jako inspiraci pro tvorbu pracovních listů) materiály z **https://o2chytraskola.cz/***

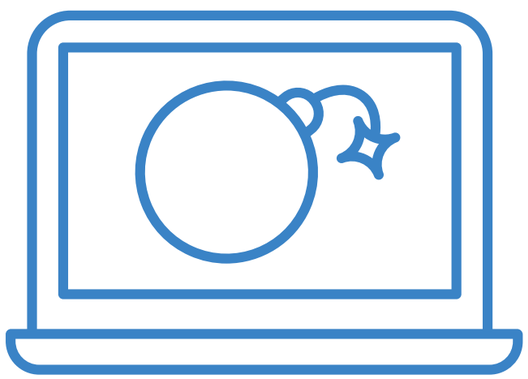
Jedná se o kvalitně zpracované materiály na témata od základního chování v online světě až po sofistikované Cyber(security+crime) materiály. Nespornou výhodou jsou již existující testy ke každému tématu chování.

Doporučené pomůcky

- Každý žák svůj počítač s (rychlým) přípojením k internetu umožňujícím paralelně streamovat videa.
- Na PC s operačním systémem Windows bude funkční prohlížeč internetových stránek.
- Sluchátka a správně nastavený zvukový výstup.
- PDF verze pracovních listů s interaktivními formuláři.
- Volitelně (pro ukládání PDF pracovních listů) 20 ks USB flashek.

Studentům řekněte, že je více než vhodné si dělat poznámky.

Pro správné zvládnutí úkolů je žádoucí mít středně pokročilou znalost anglického jazyka. Odkazy na online phishingové testy a další materiály jsou často v angličtině. I přesto, že předpokládáme, že dojde v úvodu hodiny k objasnění zadání a v pracovním listu bude také objasněno, lze tímto předejít případným dotazům. Vysvětlete studentům, že znalost anglického jazyka je pro dnešní svět (a informatiku) zásadní.



IMPULS
PRO KARIÉRU
A PRAXI