



CYBERSEC
EDUCHECK

LEKCE 1 - Phishing

Phishing: Porozumění taktikám kyberzločinců a jak zůstat v bezpečí



1



Spolufinancováno
Evropskou unií

VEDOUcí
PROJEKTU:

Coventry
University
Research Institute
Europe

PARTNERŮ:

K R
E A
STOWARZYSZENIE
KREATYWNI DLA
BIZNESU

EUROPEAN CENTRE
FOR CAREER EDUCATION



LEKCE 1 - Phishing

LEKCE 1 – Phishing

Plán výuky pro střední školy

Scénář vytvořený v rámci projektu „CyberSec EduCheck“ – projekt č. 2023-2-PL01-KA210-VET-000176822

Autoři scénáře: Weronika Kędzierska, Mateusz Pękala - Coventry University Wrocław

Věcná redaktorka: Pavla Vybíhalová - European Centre for Career Education

Grafická úprava: Karolína Kornecka-Kupiec, Jadwiga Maj - KREA Association

Wrocław 2024

Publikace je distribuována za podmínek mezinárodní licence Creative Commons Attribution NonCommercial (CC BY-NC) 4.0



LEKCE 1 - Phishing

Vážení,

poskytujeme vám plán lekce na téma phishing, což je významná hrozba v oblasti digitální bezpečnosti. Phishing patří mezi nejčastější způsoby, jak se kyberzločinci snaží získat informace. V naší lekci jsme se zaměřili na klíčové aspekty související s touto formou sociálního inženýrství.

Naše 45minutové hodiny jsou navrženy tak, aby pomohly porozumět phishingu, rozpoznat podezřelé e-maily, textové zprávy a webové stránky, a naučit se, jak na phishingové pokusy reagovat a kam takové incidenty hlásit.

Lekce jsou plánovány na krátký čas, proto se zaměříme na klíčové aktivity, jako je analýza ukázkových phishingových e-mailů a diskuse o postupech hlášení incidentů. Pokud máte více času, doporučujeme toto téma rozdělit do menších segmentů, aby bylo možné provést hlubší analýzu a lepší pochopení problematiky.

Scénář a výukové materiály, včetně prezentace, lze přizpůsobit potřebám vaší skupiny.

*S pozdravem,
Tým projektu CyberSec*

LEKCE 1 - Phishing

Obsah

Cíle lekce	3
Kontext - klíčová slova	3
Příprava na lekci	3
Struktura lekce	4
Shrnutí - k zamyšlení	5
Volitelný domácí úkol	5
Zdroje a informace pro učitele	6
Autoři a odborníci	16

LEKCE 1 - Phishing

Cíle lekce

- **Explicitní účely:**
 - Porozumět definici phishingu a technikám používaným kyberzločinci.
 - Rozpoznat podezřelé e-maily, textové zprávy a webové stránky.
 - Schopnost reagovat na phishingové pokusy a znalost postupů pro hlášení incidentů.
- **Skryté cíle:**
 - Rozvoj analytického a kritického myšlení při hodnocení zpráv a webových stránek.
 - Posílení komunikačních dovedností sdílením zkušeností a znalostí o phishingu.
 - Zvýšení povědomí o osobní bezpečnosti na internetu a odpovědnosti za ochranu osobních údajů.

Kontext - klíčová slova

phishing, digitální bezpečnost, techniky sociálního inženýrství, odpovědnost

- **Odůvodnění výběru tématu:**
 - Phishing je jednou z nejčastějších hrozeb na internetu, která může vést ke krádeži identity, ztrátě dat a finančním ztrátám.
 - Porozumění phishingovým technikám a schopnost je rozpoznat jsou klíčové pro ochranu osobních údajů a digitální bezpečnosti.
 - Vzdělávání o phishingu umožňuje nejen zvýšit povědomí o hrozbách, ale také rozvíjet kritické myšlení a odpovědnost v online prostředí.
 - Formování postojů, jako je ostražitost a schopnost reagovat na phishingové pokusy, přispívá k větší bezpečnosti na internetu a podporuje budování bezpečnějšího digitálního prostoru.

LEKCE 1 - Phishing

Příprava na lekci

- **Materiály:**

- Multimediální prezentace [Phishing – jak kyberzločinci podvádějí a jak se bránit].
- Pracovní listy s cvičeními.
- Tabule (tradiční nebo interaktivní).

- **Zkušenosti:**

o Aktivita před lekcí: Použijte úvodní činnost k uvedení studentů do tématu phishingu, využijte prvek překvapení a zapojte je do zážitkové aktivity. Příklady:

„Důležitá zpráva od učitele“. Postup: Pošlete studentům e-mail (nebo zobrazte na tabuli/projektoru) zprávu od „učitele“, která je žádá o kliknutí na odkaz, např. k vyplnění „průzkumu o škole“. Odkaz povede na falešnou webovou stránku (např. formulář s vtipnými otázkami).

„Ztracený USB disk“. Postup: Položte USB disk na viditelné místo s popiskem, např. „Známky studentů – přísně tajné“, a sledujte, kdo ho zvedne. Po chvíli vysvětlíte, že jde o příklad „hardwarového phishingu“.

„Falešná SMS od ředitele“. Postup: Zobrazte na obrazovce SMS zprávu: „Od ředitele: Žáci třídy X jsou požádáni, aby potvrdili svou účast kliknutím na odkaz: [odkaz]“.

„Přihlášení k falešné Wi-Fi síti“. Postup: Před lekcí vyvěste ceduli s nápisem „Nová Wi-Fi síť: Free_School_WiFi“ s heslem a sdělte studentům, že jde o bezplatný internet. Po několika minutách vysvětlíte, že jde o „příklad phishingu pomocí falešné Wi-Fi sítě“.

- **Prostor:**

- Uspořádání lavic tak, aby umožňovalo práci ve skupinách nebo individuálně.

LEKCE 1 - Phishing

Struktura lekce

Účel	Aktivita	Čas	Materiály
Úvod	<p>Představení tématu lekce: phishing a sociální inženýrství.</p> <p>Vysvětlení cílů lekce: Seznámení se s typy hrozeb. Schopnost rozpoznat phishingové pokusy. Naučit se metody obrany proti phishingu.</p>	5 min	Prezentace, tabule
Předání znalostí	<p>Typy hrozeb:</p> <p>Phishing: Phishing prostřednictvím falešných e-mailů, SMS (smishing) atd.</p> <p>Sociální inženýrství: Manipulační techniky používané k oklamání uživatele.</p>	10 min	Prezentace, multimediální ukázky
Praktická cvičení	<p>Rozpoznání phishingu – Pracovní list 1:</p> <p>Pracujte ve skupinách na úkolu rozpoznávání phishingových pokusů.</p> <p>Phishingový simulátor – použit k vytvoření pracovního listu 1.</p> <p>https://caniphish.com/email-phishing-simulator?email=Gmail-Blocked-Login#emailTitle</p> <p>Přehled výsledků:</p> <p>Prezentace výsledků práce skupin.</p> <p>Diskuze o použitých kritériích a vysvětlení obtížnějších problémů.</p> <p>Skupinová diskuze:</p> <p>Otázky pro podporu diskuze:</p> <p>Které prvky byly nejpřesvědčivější v analyzovaných phishingových pokusech?</p>	15 min	Pracovní listy, počítače/tablety

LEKCE 1 - Phishing

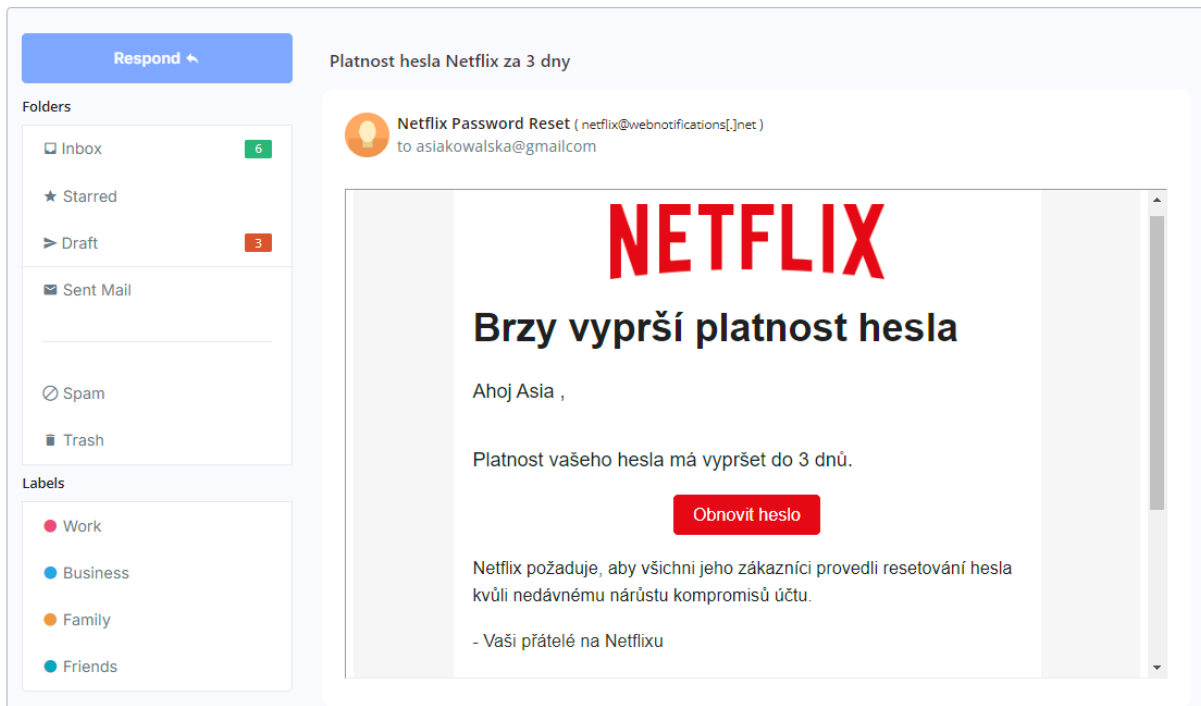
	<p>Jaké techniky sociálního inženýrství byly použity a proč?</p> <p>Co vám pomohlo rozpoznat phishingový pokus?</p>		
<p>Diskuze k výsledkům</p> <p>Rozpoznání phishingu</p>	<p>Kritéria: Přirozená návnada, zvědavost, zpoždění doručení, zpráva o výhře, rychlá akce, jazykové chyby, strach z poplatků, neobvyklé jméno odesílatele, neoficiální odkaz.</p>	10 min	Tabule, poznámky
<p>Shrnutí a zamyšlení</p>	<p>Pozvánka k testování pomocí nástroje: https://phishingquiz.withgoogle.com/</p> <p>Shrnutí klíčových problémů:</p> <p>Zopakování nejdůležitějších informací o rozpoznání a obraně proti phishingu.</p> <p>Zdůraznění role vědomého používání elektronické komunikace.</p> <p>Zamyšlení nad tématem:</p> <p>Podnět k přemýšlení, jak se chránit před phishingem v každodenním životě.</p> <p>Bezpečnost telefonu:</p> <p>Zdůraznění, že telefon je také počítač, a diskuse o zásadách zabezpečení mobilních zařízení.</p>	5 min	Prezentace

Zdroje a informace pro učitele

Vzdělávací weby a portály

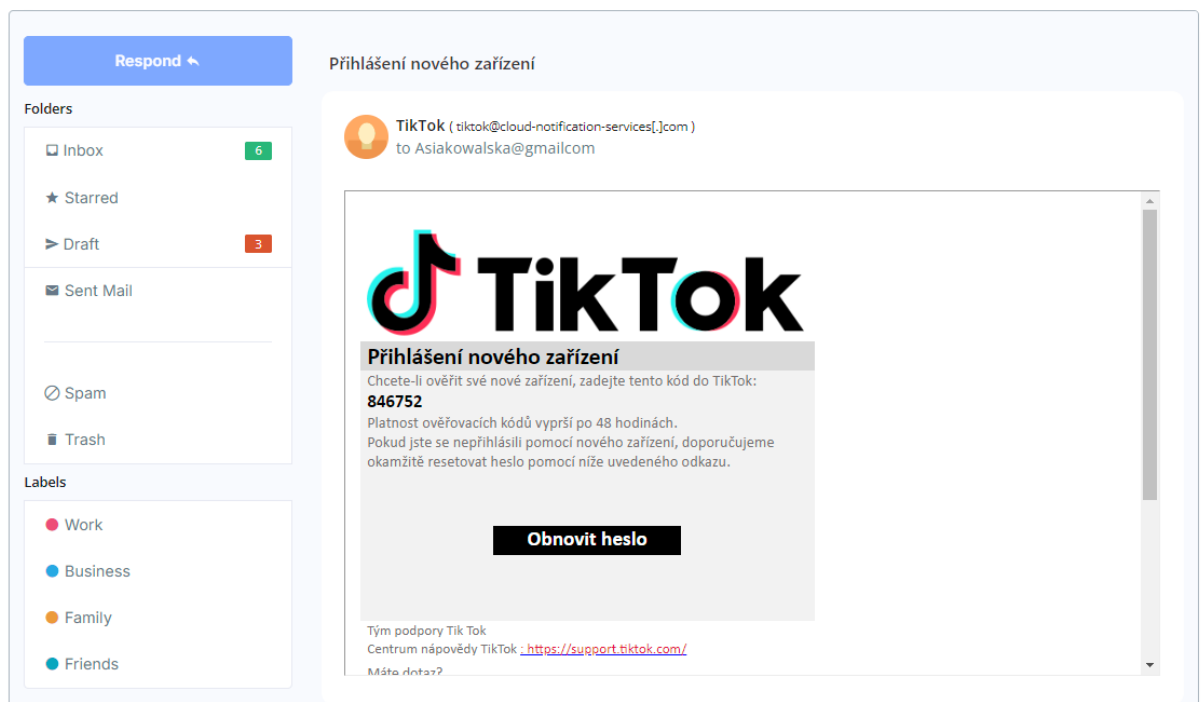
https://nukib.gov.cz/download/publikace/doporuceni/Doporuceni_spear_phishing_2.0.pdf

LEKCE 1 - Phishing



The screenshot shows an email interface with a sidebar on the left containing folders (Inbox with 6 items, Draft with 3 items, Sent Mail, Spam, Trash) and labels (Work, Business, Family, Friends). The main content area displays an email titled "Platnost hesla Netflix za 3 dny" from "Netflix Password Reset (netflix@webnotifications[.]net) to asiakowalska@gmailcom". The email body features the Netflix logo, the heading "Brzy vyprší platnost hesla", a greeting "Ahoj Asia,", and a message: "Platnost vašeho hesla má vypršet do 3 dnů." Below this is a red button labeled "Obnovit heslo". The text continues: "Netflix požaduje, aby všichni jeho zákazníci provedli resetování hesla kvůli nedávnému nárůstu kompromisů účtu." and ends with "- Vaši přátelé na Netflixu".

Zdroj: <https://caniphish.com/email-phishing-simulator?email=Gmail-Blocked-Login#emailTitle>




The screenshot shows an email interface similar to the first one. The sidebar contains the same folders and labels. The main content area displays an email titled "Přihlášení nového zařízení" from "TikTok (tiktok@cloud-notification-services[.]com) to Asiakowalska@gmailcom". The email body features the TikTok logo, the heading "Přihlášení nového zařízení", and the text: "Chcete-li ověřit své nové zařízení, zadejte tento kód do TikTok: **846752**". It continues: "Platnost ověřovacích kódů vyprší po 48 hodinách. Pokud jste se nepřihlásili pomocí nového zařízení, doporučujeme okamžitě resetovat heslo pomocí níže uvedeného odkazu." Below this is a black button labeled "Obnovit heslo". At the bottom, it says "Tým podpory Tik Tok" and "Centrum nápovědy TikTok: <https://support.tiktok.com/>".

LEKCE 1 - Phishing

Respond ←

Heslo pro váš účet 1Password bylo změněno

1Password (hello[,] password@webnotifications[.]net)
to asiakowalska@gmail.com



Ahoj Asia Kowalska,


Heslo pro váš účet 1Password bylo změněno.
Pokud jste heslo nezměnili, [kliknutím sem tuto změnu](#) v příštím 24 hodin změníte.

1Password
vyrobil 1Password • odesláno na: asiakowalska@gmail.com
4711 Yonge St. 10. patro • Toronto • Ontario • M2N 6K3 • Kanada

Respond ←

Nové přihlášení do Instagramu z prohlížeče Chrome ve Windows


Instagram Notifications (instagram@webnotifications[.]net)
to asiakowalska@gmail.com



Instagram

Asia, všimli jsme si nového přihlášení.

Všimli jsme si přihlášení ze zařízení, které obvykle nepoužíváte.



Okna · Chrom · Bangkok, Thajsko
Tue Sep 17 2024 12:17:36 GMT+0200 (čas
šrodkowoeuropejski letni) (PDT)

Kdybys to byl ty, tento e-mail můžete bezpečně ignorovat. Pokud jste to nebyl vy, můžete si svůj účet zabezpečit [zde](#).


[Další informace](#) o zabezpečení vašeho účtu.

LEKCE 1 - Phishing

Respond ↩

Žádost o obnovení hesla

Slack (slack@webnotifications[.]net)
to asiakowalska@gmail.com



Obnovení hesla pracovního prostoru Slack

Požádali jste nás o zaslání odkazu na obnovení hesla pro auth.slack.com. Tento požadavek na obnovení hesla je určen pro asiakowalska@gmail.com.

Pokud jste tento požadavek na obnovení hesla neautorizovali, **informujte** prosím tým na slack.

Tento odkaz na obnovení hesla bude platný dalších 24 hodin a je vázán na e-mailovou adresu: asiakowalska@gmail.com. Pokud máte nějaké problémy, obraťte se na svého správce o podporu.

Obnovit heslo

Folders

- Inbox 6
- Starred
- Draft 3
- Sent Mail
- Spam
- Trash

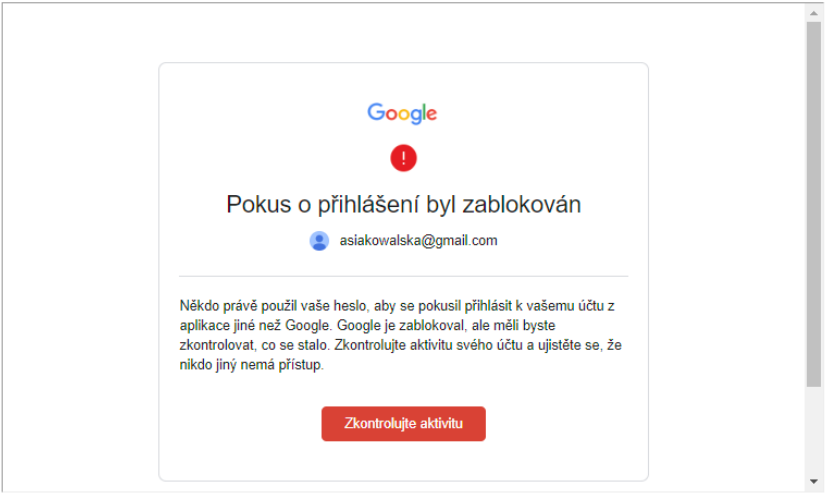
Labels

- Work
- Business
- Family
- Friends

Respond ↩

Bezpečnostní upozornění: Pokus o přihlášení zablokován.

Google Notifications (google-support@webnotifications[.]net)
to asiakowalska@gmail[.]com



Pokus o přihlášení byl zablokován

asiakowalska@gmail.com

Někdo právě použil vaše heslo, aby se pokusil přihlásit k vašemu účtu z aplikace jiné než Google. Google je zablokoval, ale měli byste zkontrolovat, co se stalo. Zkontrolujte aktivitu svého účtu a ujistěte se, že nikdo jiný nemá přístup.

Zkontrolujte aktivitu

Folders

- Inbox 6
- Starred
- Draft 3
- Sent Mail
- Spam
- Trash

Labels

- Work
- Business
- Family
- Friends

LEKCE 1 - Phishing

Autoři a odborníci



Weronika Kędzierska – expertka v oblasti měkkých aspektů kyberbezpečnosti, zaměřující se na vytváření bezpečné základny kyberbezpečnosti pro mladé organizace. Specializuje se na rozvoj efektivních týmů, organizační změny a implementaci inovačních strategií. Jako nezávislá konzultantka a koučka pomáhá lídrům a týmům budovat zapojení a spolupráci. Je oceňována za kreativní a hodnotné workshopy, které efektivně inspirují týmy k dosahování jejich cílů.



Mateusz Pękala – specialista na zvyšování povědomí o bezpečnosti informací, security compliance, audity informační bezpečnosti a řízení rizik. Má dlouholeté zkušenosti jako auditor, školitel a konzultant v oblasti informační bezpečnosti. Je členem profesionálních organizací, jako jsou ISSA Poland a ISACA. Vlastní certifikace Certified in Risk and Information Systems Control™ (CRISC), Certified Information Security Professional (CISSP), Certified Data Privacy Solutions Engineer™ (CDPSE)® a Certified Information Systems Auditor® (CISA), a je také certifikovaným auditorem v oblasti ISO 27001.



LEKCE 1 - Phishing

Více informací o projektu

Financováno Evropskou unií. Vyjádřené názory a názory jsou však výhradně názory autora (autorů) a nemusí nutně odrážet názory Evropské unie nebo Evropské výkonné agentury pro vzdělávání a kulturu (EACEA). Evropská unie ani EACEA za ně nemohou nést odpovědnost.

Všechny výsledky vytvořené v rámci tohoto projektu jsou dostupné pod otevřenými licencemi (CC BY-NC 4.0). Lze je používat zdarma a bez omezení. Kopírování nebo zpracování těchto materiálů jako celku nebo jejich částí bez souhlasu autora je zakázáno. V případě využití výsledků je nutné uvést zdroj financování a jejich autory.

PROJEKT Č. 2023-2-PL01-KA210-VET-000176822

- <https://www.coventry.ac.uk/wroclaw/>
- <https://kreatywnidlabiznesu.pl/cyber-sec-edu-check/>
- <https://eccedu.net/>

