cesnet

Sociální inženýrství a phishing II.

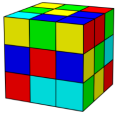
Aleš Padrta

apadrta@cesnet.cz

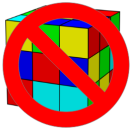
Cvičné phishingové zprávy

cesnet

- Teoretická přednáška
  - Videokonferenčně, kávička, pohodlí, . . .
  - Nehrozí žádné nebezpečí
  - Všechno je zřejmé (logické)



- Phishing ve vlastní schránce
  - Vliv sociálního inženýrství
  - Amygdala v akci



- Cvičné zprávy
  - Trénink reakce (zkrocení amygdaly)
  - Bez nebezpečí pro adresáty (důvěryhodná realizace)
  - Snazší odolat skutečnému útoku

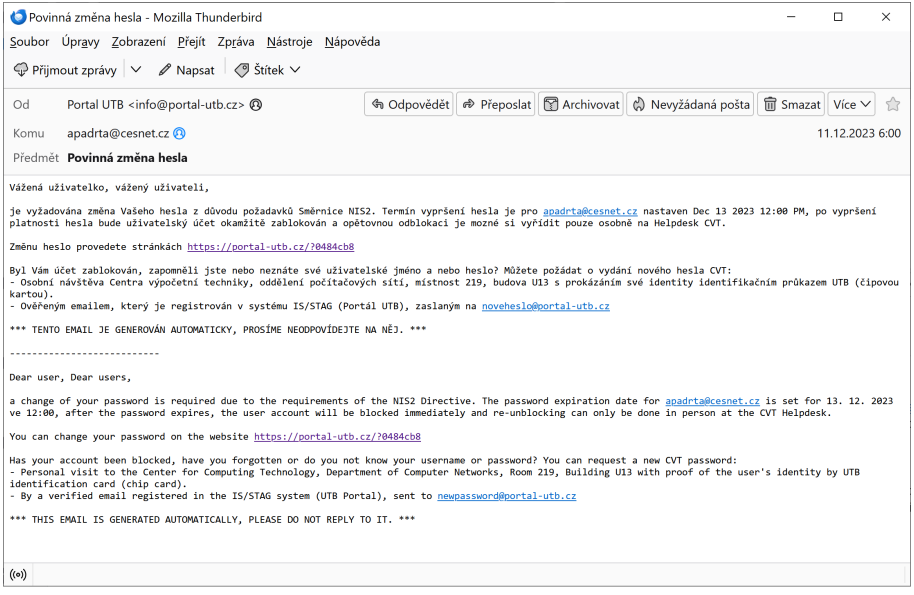
Phishing ze dne 11. 12. 2023

Příprava cvičné zprávy

cesnet

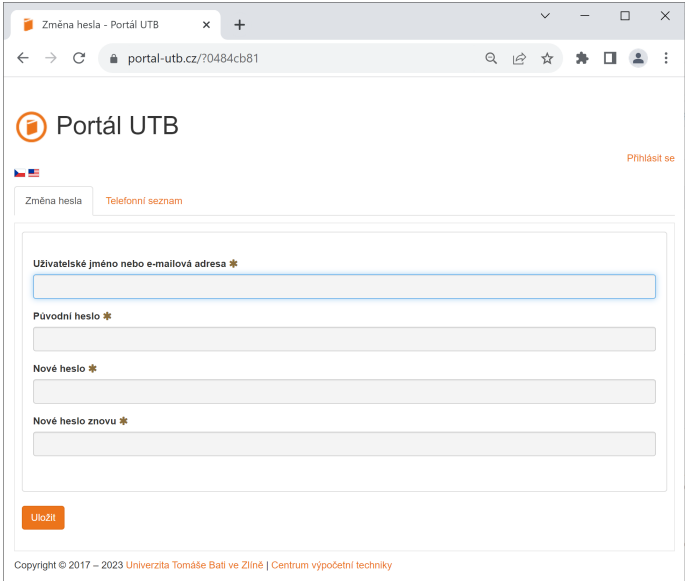
- Simulace podvodu ⇒ myšlení podvodníka
- Volba přihlašovací stránky
  - Změna hesla (staré i nové heslo najednou? podvodník by jásal)
- Volba podvodné domény – podobná originálu
  - Správná **portal.utb.cz**
  - Podvodná **portal-utb.cz**
- Téma – aktuální dění
  - Směrnice NIS2 – účinnost od ledna (věrohodné řešit v prosinci)
- Záminka
  - Splnění podmínek NIS2
  - Nutná změna hesla (nové požadavky směrnice?)

Zaslaná zpráva

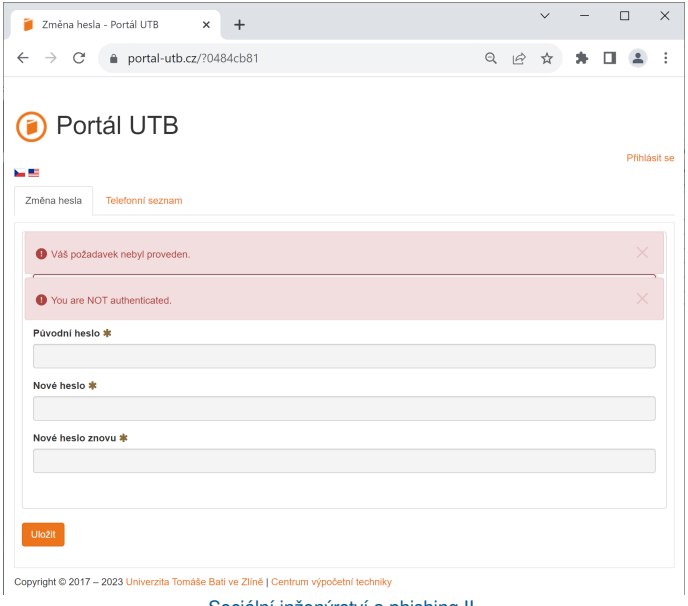


Odkazovaný web `portal-utb.cz`

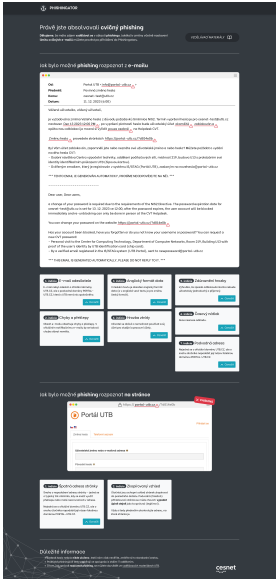
cesnet



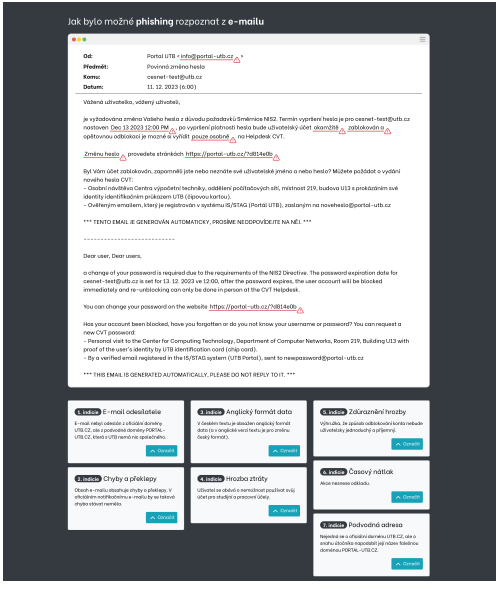
Kontrola platnosti



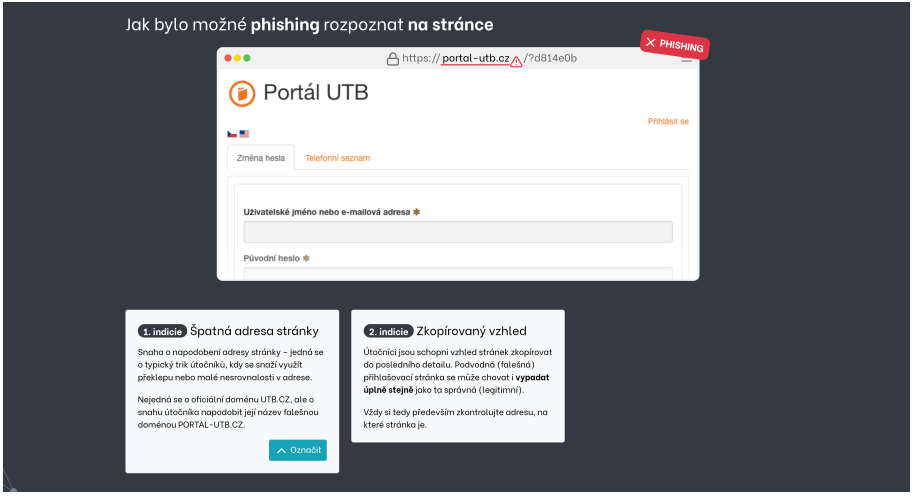
Realizace – Vzdělávací stránka



Realizace – Vzdělávací stránka



Realizace – Vzdělávací stránka



Vyhodnocení

Výsledky

cesnet

- Cvičný phishing v číslech
  - 2096 obeslaných uživatelů
  - 9 out of office zpráv
  - 9 odpovědí na zprávu
  - 384 návštěv podvodného webu
  - 266 zadání údajů do podvodného webu
  - 244 platných přihlašovacích údajů
- Celková úspěšnost cvičného phishing – 11,6 %
  - Věrohodná záminka
  - Povedená doména
  - Načasování – konec roku, stresování

Hlášení

cesnet

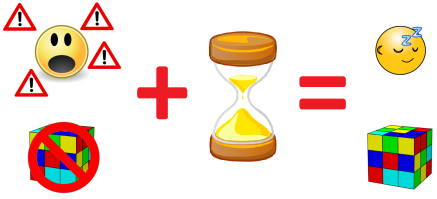
- Hlášení podvodných zpráv / konzultace – IT oddělení
  - Pomoc – „určitě nevím, jestli je to podvod“
  - Zjištění probíhajícího útoku
  - Technické prostředky – blokování přístupu / dohledání
  - Ochrana ostatních kolegyň a kolegů
- Hlášení během cvičné phishingové kampaně
  - První phishingový e-mail – 6:00
  - První hlášení – 6:07
  - Reakce do 10 minut $\Rightarrow$ 232 ochráněných účtů
    (útočník by získal jen 12)
  - Celkem 81 hlášení (3,86 %)

Shrnutí

- Sociální inženýrství a phishing

  $\Rightarrow$ oblíbený trik kyberpodvodníků
- Obrana
  - Znalost triků
  - Školení + praktická ukázka
  - Rozpoznání podvodu
- Dobré rady na závěr
  - Kontrola domény

    (zadávání přihlašovacích údajů)
  - Konzultace/hlášení $\rightarrow$ IT oddělení
  - Čas na rozmyšlenou



cesnet

Dotazy a diskuse