

Sociální inženýrství a phishing II.

Aleš Padrta

apadrta@cesnet.cz

- Teoretická přednáška

- ▶ Videokonferenčně, kávačka, 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

- Simulace podvodu \Rightarrow myšlení podvodníka
- Volba přihlašovacích 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?)

Povinná změna hesla - Mozilla Thunderbird

Soubor Úpravy Zobrazení Přejít Zpráva Nástroje Nápověda

Přijmout zprávy Napsat Štítek

Od Portal UTB <info@portal-utb.cz> Odpovědět Přeposlat Archivovat Nevyžádaná pošta Smazat Více

Komu apadrta@cesnet.cz 11.12.2023 6:00

Předmět **Povinná změna hesla**

Vážená uživatelko, vážený uživateli,

je vyžadována změna Vašeho hesla z důvodu požadavků Směrnice NIS2. Termín vypršení hesla je pro apadrta@cesnet.cz nastaven Dec 13 2023 12:00 PM, po vypršení platnosti hesla bude uživatelský účet okamžitě zablokován a opětovnou odblokaci je možné si vyřídit pouze osobně na Helpdesk CVT.

Změnu heslo provedete stránkách <https://portal-utb.cz/?0484cb8>

Byl Vám účet zablokován, zapoměli jste nebo neznáte své uživatelské jméno a nebo heslo? Můžete požádat o vydání nového hesla CVT:

- Osobní návštěva Centra výpočetní techniky, oddělení počítačových sítí, místnost 219, budova U13 s prokázáním své identity identifikačním průkazem UTB (čipovou kartou).
- Ověřeným emailem, který je registrován v systému IS/STAG (Portál UTB), zaslaným na noveheslo@portal-utb.cz

*** TENTO EMAIL JE GENEROVÁN AUTOMATICKY, PROSÍME NEODPOVÍDEJTE NA NĚJ. ***

Dear user, Dear users,

a change of your password is required due to the requirements of the NIS2 Directive. The password expiration date for apadrta@cesnet.cz is set for 13. 12. 2023 ve 12:00, after the password expires, the user account will be blocked immediately and re-unblocking can only be done in person at the CVT Helpdesk.

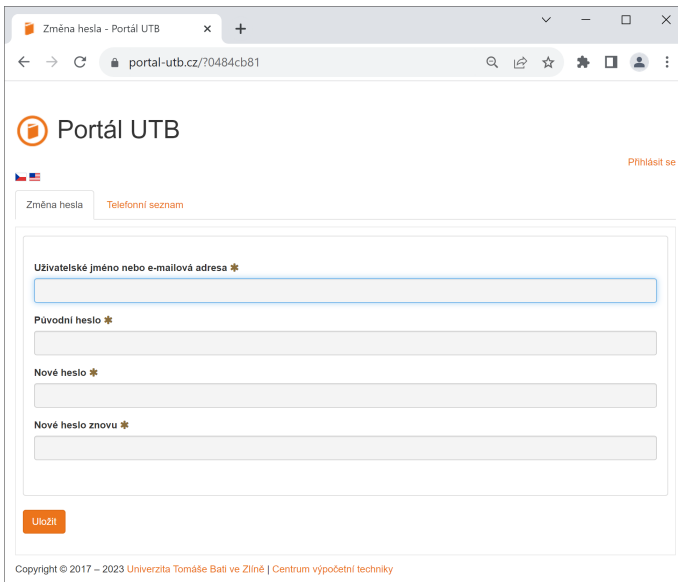
You can change your password on the website <https://portal-utb.cz/?0484cb8>

Has your account been blocked, have you forgotten or do you not know your username or password? You can request a new CVT password:

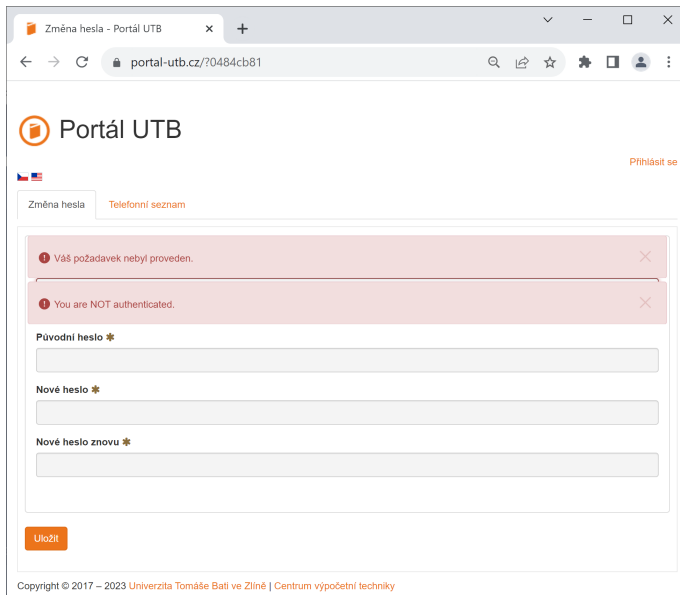
- Personal visit to the Center for Computing Technology, Department of Computer Networks, Room 219, Building U13 with proof of the user's identity by UTB identification card (chip card).
- By a verified email registered in the IS/STAG system (UTB Portal), sent to newpassword@portal-utb.cz

*** THIS EMAIL IS GENERATED AUTOMATICALLY, PLEASE DO NOT REPLY TO IT. ***

(v)

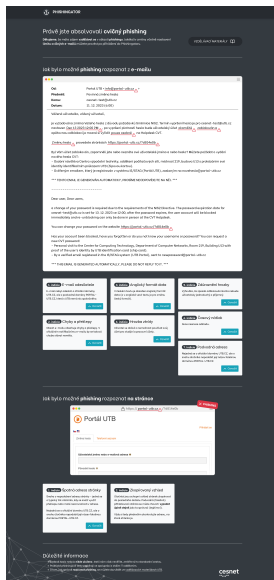


The screenshot shows a web browser window with the address bar displaying 'portal-utb.cz/?0484cb81'. The page title is 'Změna hesla - Portál UTB'. The main content area features the 'Portál UTB' logo and a 'Přihlásit se' link. Below the logo are two tabs: 'Změna hesla' (selected) and 'Telefonní seznam'. The 'Změna hesla' form contains four input fields: 'Uživatelské jméno nebo e-mailová adresa *', 'Původní heslo *', 'Nové heslo *', and 'Nové heslo znovu *'. An 'Uložit' button is located at the bottom of the form. The footer contains the text: 'Copyright © 2017 – 2023 Univerzita Tomáše Bati ve Zlíně | Centrum výpočetní techniky'.



The screenshot shows a web browser window with the address bar displaying 'portal-utb.cz/?0484cb81'. The page title is 'Změna hesla - Portál UTB'. The main content area features the 'Portál UTB' logo and a navigation menu with 'Změna hesla' (selected) and 'Telefonní seznam'. A 'Přihlásit se' link is visible in the top right. Two red error messages are displayed: 'Váš požadavek nebyl proveden.' and 'You are NOT authenticated.'. Below these are three password input fields labeled 'Původní heslo *', 'Nové heslo *', and 'Nové heslo znovu *'. An 'Uložit' button is at the bottom of the form.

Copyright © 2017 – 2023 Univerzita Tomáše Bati ve Zlíně | Centrum výpočetní techniky



Jak bylo možné phishing rozpoznat z e-mailu

Od: Portal UTB + info@portal-utb.cz
 Přijetí: Posíláno z jiného hesla
 Kому: cesnet-heat@utb.cz
 Datum: 11. 12. 2023 (6:00)

Vážená uživatelsko, vážený uživatel,

Je vyžadována změna Vašeho hesla z důvodu požadavků Směrnice NIS2. Termín vypršení hesla je pro cesnet-heat@utb.cz nastaven **Do: 13. 12. 2023 12:00**, po vypršení platnosti hesla bude uživatelský účet **okamžitě zablokován** a **opětovnou odzkoukou je možné si vyžádat pouze osobně** na Helpdesk CVT.

Změnu hesla provedete stránkách <https://portal-utb.cz/7081446>

Byl Vám účet zablokován, zapomenkl jste nebo neznáte své uživatelské jméno a nebo heslo? Můžete požádat o vydání nového hesla CVT:

- Osobně u odběrnáka Centra výpočetní techniky, oddělení počítačových sítí, místnost 219, budova U13 a prokázáním své identity identifikacími průkazem UTB (špičková karta).
- Ověřeným emailem, který je registrován v systému IS/STAG (Portál UTB), zasláním na novéheslo@portal-utb.cz

*** TENTO EMAIL JE GENEROVÁN AUTOMATICKY, PROSÍME NEODPOVÍDEJTE NA NĚ! ***

Dear user, Dear users,

a change of your password is required due to the requirements of the NIS2 Directive. The password expiration date for cesnet-heat@utb.cz is set for 13. 12. 2023 at 12:00, after the password expires, the user account will be blocked immediately and re-unblocking can only be done in person at the CVT Helpdesk.

You can change your password on the website <https://portal-utb.cz/7081446>

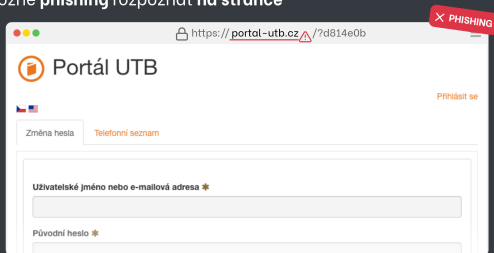
Has your account been blocked, have you forgotten or do you not know your username or password? You can request a new CVT password:

- Personally visit to the Center for Computing Technology, Department of Computer Networks, Room 219, Building U13 with proof of the user's identity by UTB identification card (chip card).
- By a verified email registered in the IS/STAG system (UTB Portal), sent to newpassword@portal-utb.cz

*** THIS EMAIL IS GENERATED AUTOMATICALLY, PLEASE DO NOT REPLY TO IT. ***

1. tip E-mail odesílatelé E-mail neply cestuje z adresy domény UTB.CZ, ale z adresy domény PSEKAL, UTB.CZ, která s UTB nemá nic společného. Otevřít	2. tip Anglický formát data V zasedání byly je obsažen anglický formát data (a anglické heslo) je pro změnu český formát. Otevřít	3. tip Zákazníkem/hrozby Vzhledem, že způsob odzkoušení krevu nebyl uživatelský, jedná se o hrozbu. Otevřít
3. tip Chyby a překlepy Obsah e-mailu obsahuje chyby a překlepy. V případě em-out@hrozbacv.cz e-mail by se taková chyba objevit neměla. Otevřít	4. tip Hrozba ztráty Uživatel se obává o nemožnost používat svůj účet pro studijní a pracovní účely. Otevřít	4. tip Časový nátlak Alike nemožnost odzkou. Otevřít
5. tip Podvodná adresa Zjednotil se o adresě domény UTB.CZ, ale o smyslu zablokování nepožádal ani název telefonní domény PSEKAL-UTB.CZ. Otevřít		

Jak bylo možné **phishing** rozpoznat na stránce



1. indicie Špatná adresa stránky

Snaha o napodobení adresy stránky - jedná se o typický trik útočníků, kdy se snaží využít překlepu nebo malé nesrovnalosti v adrese.

Nejedná se o oficiální doménu UTB.CZ, ale o snahu útočníka napodobit její název falešnou doménou PORTAL-UTB.CZ.

^ Označit

2. indicie Zkopírovaný vzhled

Útočníci jsou schopni vzhled stránek zkopírovat do posledního detailu. Podvodná (falešná) přihlašovací stránka se může chovat i **vypadat úplně stejně** jako ta správná (legitimní).

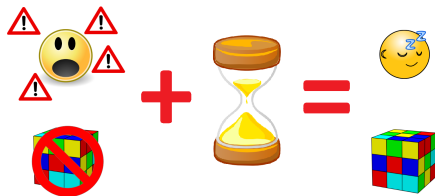
Vždy si tedy především zkontrolujte adresu, na které stránka je.

Vyhodnocení

- 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 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 %)

- Sociální inženýrství a phishing
 - ⇒ oblíbený trik kyberpodvodníků
- Obrana
 - ▶ Znalost triků
 - ▶ Školení + praktická ukázka
 - ▶ Rozpoznání podvodu
- Dobré rady na závěr
 - ▶ Kontrola domény (zadávání přihlašovacích údajů)
 - ▶ Konzultace/hlášení → IT oddělení
 - ▶ Čas na rozmyšlenou



Dotazy a diskuse