SECFEST2021:$

./"Techniky sociálního inženýrství, phishing"

< Martin Šebela && 15. 11. 2021

Sociální inženýrství

- Psychologická **manipulace**
- Cílem útočníka je, **oklamat** svou oběť a **přimět** ji k provedení akce
- Založeno na **stresové situaci**, **nepozornosti**
- **Zvědavost** („Co je na tom ztraceném USB disku? Kam ten odkaz vede?“)

- Metody:
  - Poutavý příběh – vzbuzení soucitu, **emoce**
  - Vydávání se **za autoritu** (ředitele, správce webmailu, exekutora, …)
  - **Časová tíseň** (tlak na uživatele)
  - **Hrozba ztrátou**

Phishing

- *Phishing* = **podvodné e-maily**
  - Svázané s **podvodnou stránkou**
  - Obsahující **zavirovanou přílohu**

- Cílem získat citlivé údaje – **hesla**, údaje k **platební kartě** a zneužít **identitu**
- Útočníci se často **vydávají za důvěryhodné firmy** (přepravní společnosti, banky, …)
  - Nevyzvednutý balíček, nezaplacená faktura, …

- *Spear phishing* = **cílený** phishing

Vishing

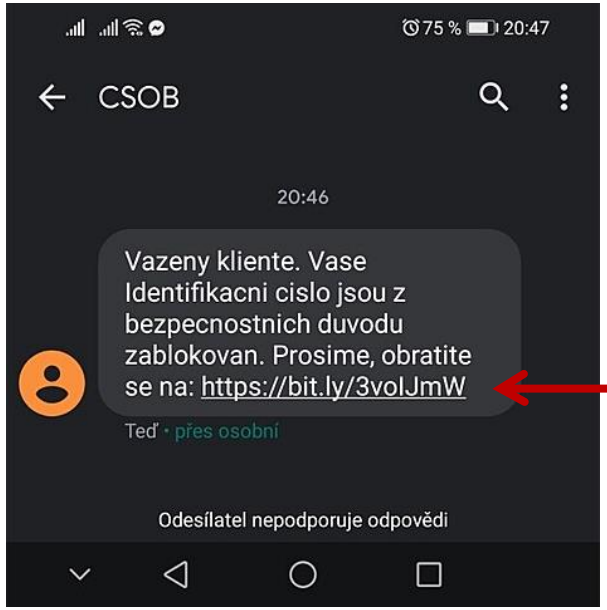
- *Vishing* = voice-phishing, **phishing po telefonu**
- Cílem vyvolat **strach**, naléhavost a **zpanikaření**
- Získání důvěry díky **veřejně dostupným informacím** o oběti – sociální sítě
- **Spoofing** telefonního čísla
- Vedení hovoru jako u callcentra

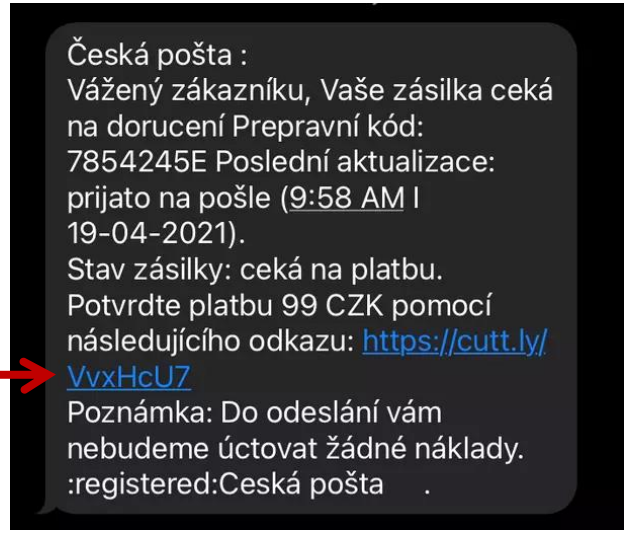
- V nočních nebo brzkých ranních hodinách
  - Člověk není tolik **obezřetný**
  - **Příklad:** Požadováno číslo **platební karty**, platnost, CV a **potvrzovací kód z SMS**
    - seznamzpravy.cz/clanek/autenticka-nahravka-zlodeje-takhle-vas-okrade-o-citlive-udaje-a-penize-156431
    - nukib.cz/cs/infoservis/aktuality/1699-upozorneni-na-podvodne-telefonaty-od-falesne-technicke-podpory-microsoft/

Smishing

- *Smishing* = phishing prostřednictvím **textové** nebo **SMS zprávy**
- Ve zprávě je odkaz na **podvodnou stránku**

- **Příklady:**
  - SMS o zablokování bankovního účtu
  - SMS o doručení balíčku

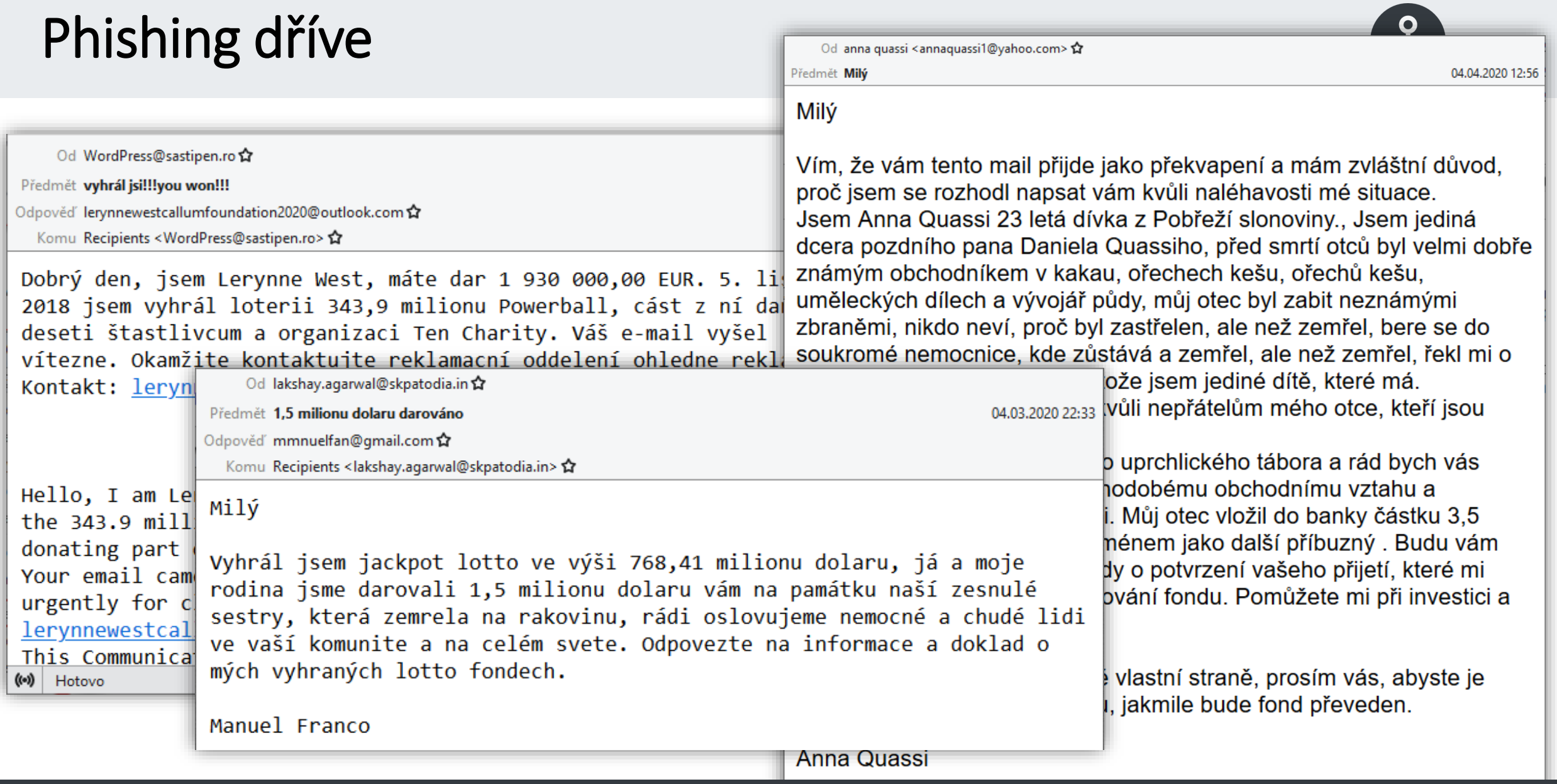




Odkazy na podvodné stránky

- idnes.cz/mobil/mobilni-operatori/podvodna-sms-phishing-internetove-bankovnictvi-csob-banka-podvod.A210616_103351_mobilni-operatori_LHR
- seznamzpravy.cz/clanek/kvuli-podvodu-prisla-o-desetitisice-jaka-nebezpeci-na-vas-cihaji-v-mobilu-155173

Phishing dříve



Od WordPress@sastipen.ro
Předmět **vyhrál jsi!!!you won!!!**
Odpověď lerynnewestcallumfoundation2020@outlook.com
Komu Recipients <WordPress@sastipen.ro>

Dobrý den, jsem Lerynne West, máte dar 1 930 000,00 EUR. 5. li
2018 jsem vyhrál loterii 343,9 milionu Powerball, část z ní da
deseti štastlivcum a organizaci Ten Charity. Váš e-mail vyšel
vítezne. Okamžite kontaktujte reklamacní oddelení ohledne rekl
Kontakt: leryn

Hello, I am Le
the 343.9 mill
donating part
Your email cam
urgently for c
lerynnewestcal
This Communica

Hotovo

Od lakshay.agarwal@skpatodia.in
Předmět **1,5 milionu dolaru darováno** 04.03.2020 22:33
Odpověď mmnuelfan@gmail.com
Komu Recipients <lakshay.agarwal@skpatodia.in>

Milý

Vyhrál jsem jackpot lotto ve výši 768,41 milionu dolaru, já a moje rodina jsme darovali 1,5 milionu dolaru vám na památku naší zesnulé sestry, která zemrela na rakovinu, rádi oslovujeme nemocné a chudé lidi ve vaší komunite a na celém svete. Odpovezte na informace a doklad o mých vyhraných lotto fondech.

Manuel Franco

Od anna quassi <annaquassi1@yahoo.com>
Předmět **Milý** 04.04.2020 12:56

Milý

Vím, že vám tento mail přijde jako překvapení a mám zvláštní důvod, proč jsem se rozhodl napsat vám kvůli naléhavosti mé situace. Jsem Anna Quassi 23 letá dívka z Pobřeží slonoviny., Jsem jediná dcera pozdního pana Daniela Quassiho, před smrtí otců byl velmi dobře známým obchodníkem v kakau, ořechech kešu, ořechů kešu, uměleckých dílech a vývojář půdy, můj otec byl zabit neznámými zbraněmi, nikdo neví, proč byl zastřelen, ale než zemřel, bere se do soukromé nemocnice, kde zůstává a zemřel, ale než zemřel, řekl mi o
ože jsem jediné dítě, které má.
vůli nepřátelům mého otce, kteří jsou

o uprchlického tábora a rád bych vás
nodobému obchodnímu vztahu a
i. Můj otec vložil do banky částku 3,5
ménem jako další příbuzný . Budu vám
dy o potvrzení vašeho přijetí, které mi
ování fondu. Pomůžete mi při investici a

vlastní straně, prosím vás, abyste je
, jakmile bude fond převeden.

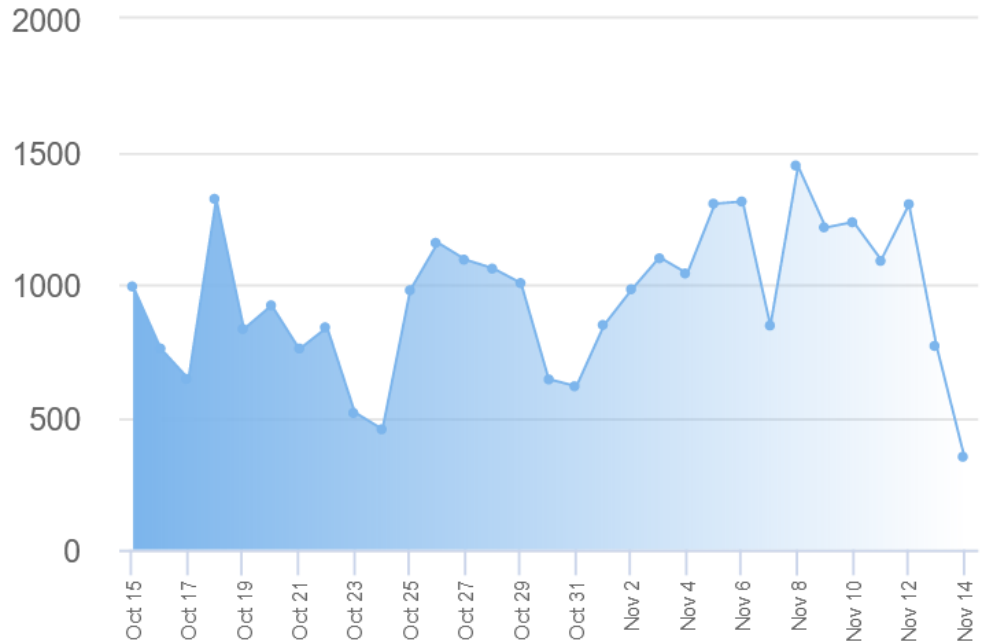
Anna Quassi

Phishing dnes

- Phishing, který napodobuje **banky**, **přepravní společnosti**, …
  - Svázaný s **podvodnou webovou stránkou**
  - Obsahující **zavirovanou přílohu**

- Podvodné stránky **věrně napodobují** skutečné stránky společností
- Podvodné stránky často běží na **protokolu HTTPS**
- Podvodné stránky mohou být odeslány jako **HTML příloha** (2021)

Počty nahlášených phishingových stránek na *PhishTank* (období říjen–listopad 2021)

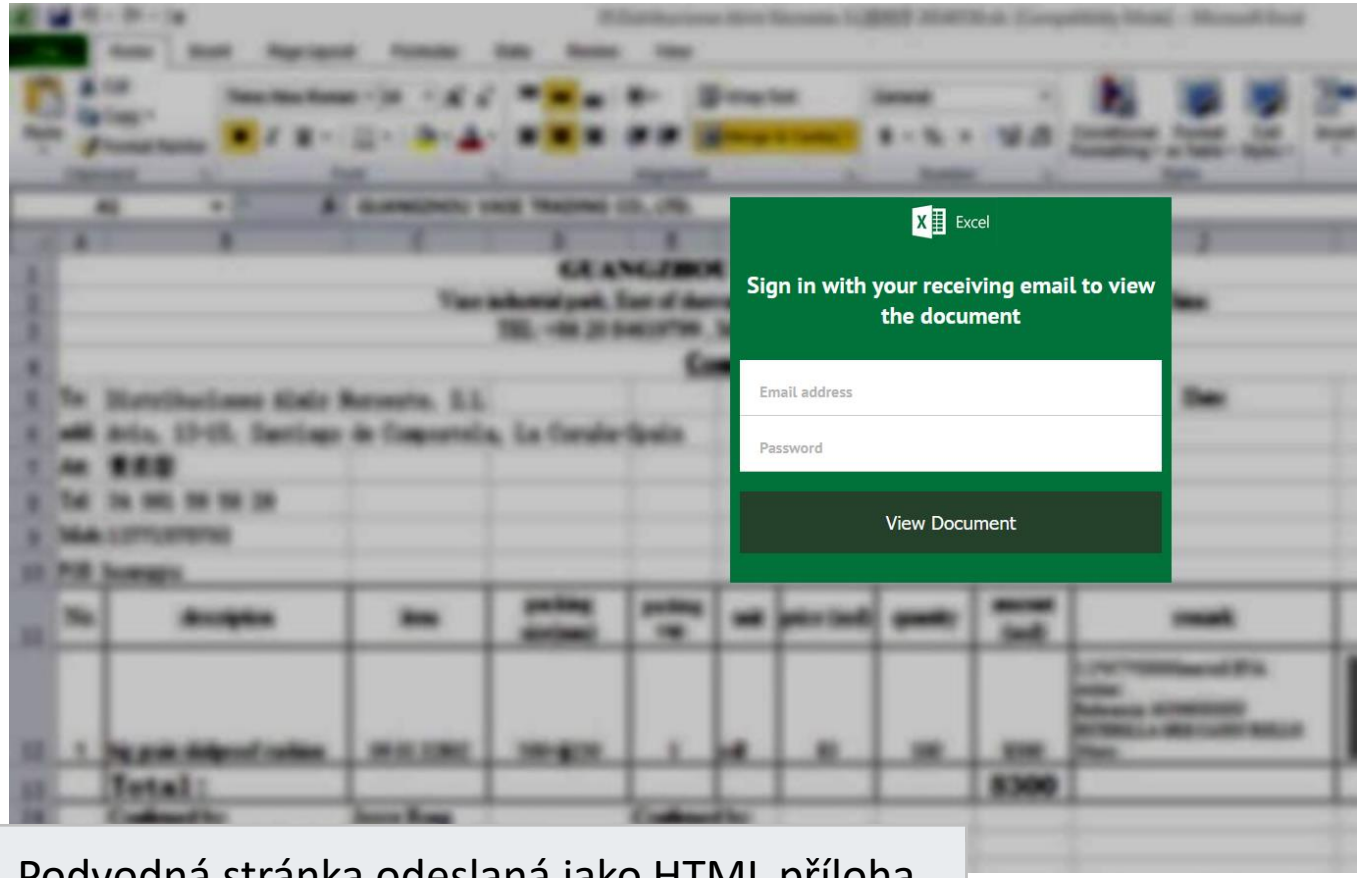


phishtank.com/stats.php

Phishing – podvodné stránky

- Podvodné stránky odesílané jako **HTML příloha** (2021)
  - Není potřeba hostitele
  - Může být zakódováno *base64*
  - Vyplněný formulář odesílán na vzdálený server

- **Příklad:** Nezaplacená faktura od DHL s HTML přílohou
  - V pozadí obrázek faktury – *„přihlaste se Office identitou“*
  - Odesláním formuláře dojde k uložení dat do služby *jotform.com*
  - Phishing ze srpna 2021



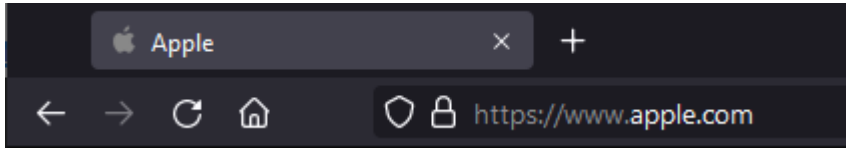
Podvodná stránka odeslaná jako HTML příloha.

Phishing – podvodné domény

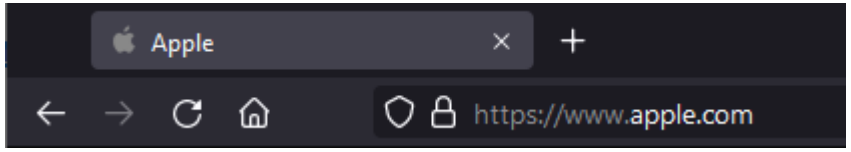
- Podvodnou stránku **lze rozpoznat podle adresy** v adresním řádku
- Útočníci se často pokouší do adresy **umístit název organizace** (firmy, univerzity, …) tak, aby adresa **vypadala důvěryhodněji**
  - `zcu.cz.oiwrnd.cz`, `zcu-cz.blogger.com/fw…ef`, … vs. `wirt.zcu.cz`

- Útočníci mohou také v podvodných doménách použít **znaky z jiných abeced**

`apple.com`



`apple.com`

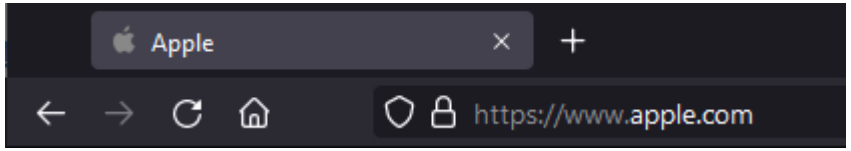


Phishing – IDN homograph attack

```
03B1 ;  0061 ;  MA      # ( α → a ) GREEK SMALL LETTER ALPHA → LATIN SMALL LE
1D6C2 ; 0061 ;  MA      # ( 𝛂 → a ) MATHEMATICAL BOLD SMALL ALPHA → LATIN SMA
1D6FC ; 0061 ;  MA      # ( 𝛼 → a ) MATHEMATICAL ITALIC SMALL ALPHA → LATIN SMALL LETTER A      # →α→
1D736 ; 0061 ;  MA      # ( 𝜶 → a ) MATHEMATICAL BOLD ITALIC SMALL ALPHA → LATIN SMALL LETTER A # →α→
1D770 ; 0061 ;  MA      # ( 𝝰 → a ) MATHEMATICAL SANS-SERIF BOLD SMALL ALPHA → LATIN SMALL LETTER A     # →α→
1D7AA ; 0061 ;  MA      # ( 𝞪 → a ) MATHEMATICAL SANS-SERIF BOLD ITALIC SMALL ALPHA → LATIN SMALL LETTER A      # →α→
0430 ;  0061 ;  MA      # ( а → a ) CYRILLIC SMALL LETTER A → LATIN SMALL LETTER A      #
```

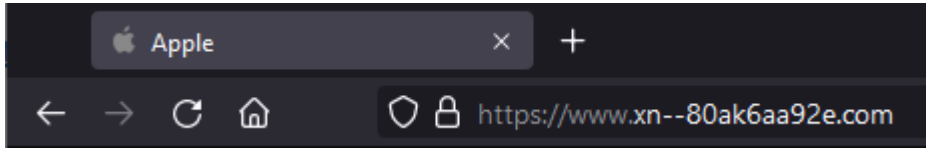
Který ze znaků se nejvíce podobá „a“?

apple.com



=

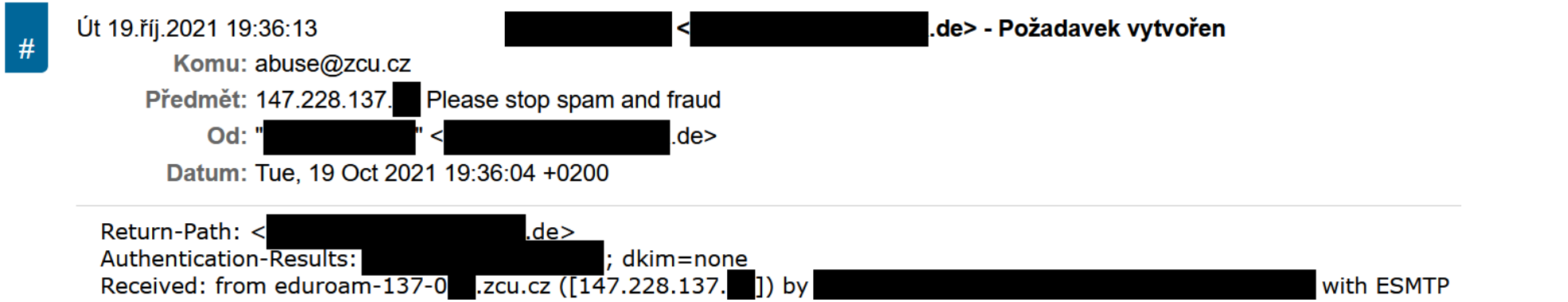
xn--80ak6aa92e.com



- Ve *Firefoxu* lze zapnout zobrazení *punycode* pomocí `network.IDN_show_punycode`

Phishing – napadená zařízení

- Rozesílání phishingu z **napadených zařízení** uživatelů
- Případ ze ZČU z října 2021:



Út 19.říj.2021 19:36:13 [redacted] <[redacted].de> - **Požadavek vytvořen**

Komu: abuse@zcu.cz

Předmět: 147.228.137.[redacted] Please stop spam and fraud

Od: "[redacted]" <[redacted].de>

Datum: Tue, 19 Oct 2021 19:36:04 +0200

Return-Path: <[redacted].de>
Authentication-Results: [redacted]; dkim=none
Received: from eduroam-137-0[redacted].zcu.cz ([147.228.137.[redacted]]) by [redacted] with ESMTP

Stížnost německé organizace na chování zařízení ze sítě ZČU.

- Z napadeného zařízení bylo během jednoho dne rozesláno 600 **phishingových e-mailů**

Reálný phishing

- Phishing **vydávající se za kalendář mezd** registrovaný několika univerzitami v ČR
- Odkaz na **podvodnou stránku**, která napodobuje univerzitní přihlašovací stránku

Kalendář plánu mezd 2021 je nyní k dispozici (důležitý)

Středa, Březen 10, 2021 11:30 CET

Komu

Západočeská univerzita caitrin.engle@webzcu.cz

msebela@civ.zcu.cz

Kalendář plánu mezd 2021 je nyní k dispozici:

- http://login.webzcu.cz/?ha0291dl

© Západočeská univerzita v Plzni

Tento e-mail byl zkontrolován programem na viry.

Reálný phishing

- Phishing **vydávající se za kalendář mezd** registrovaný několika univerzitami v ČR
- Odkaz na **podvodnou stránku**, která napodobuje univerzitní přihlašovací stránku

Cvičný phishing (ZČU)

- Na základě **skutečného phishingu** registrovaného několika univerzitami v ČR
- **Cvičný podvodný e-mail** odeslaný z *Phishingatoru* s odkazem na **podvodnou stránku**

Kalendář plánu mezd 2021 je nyní k dispozici (důležitý)

Středa, Březen 10, 2021 11:30 CET

Komu

Západočeská univerzita caitrin.engle@webzcu.cz

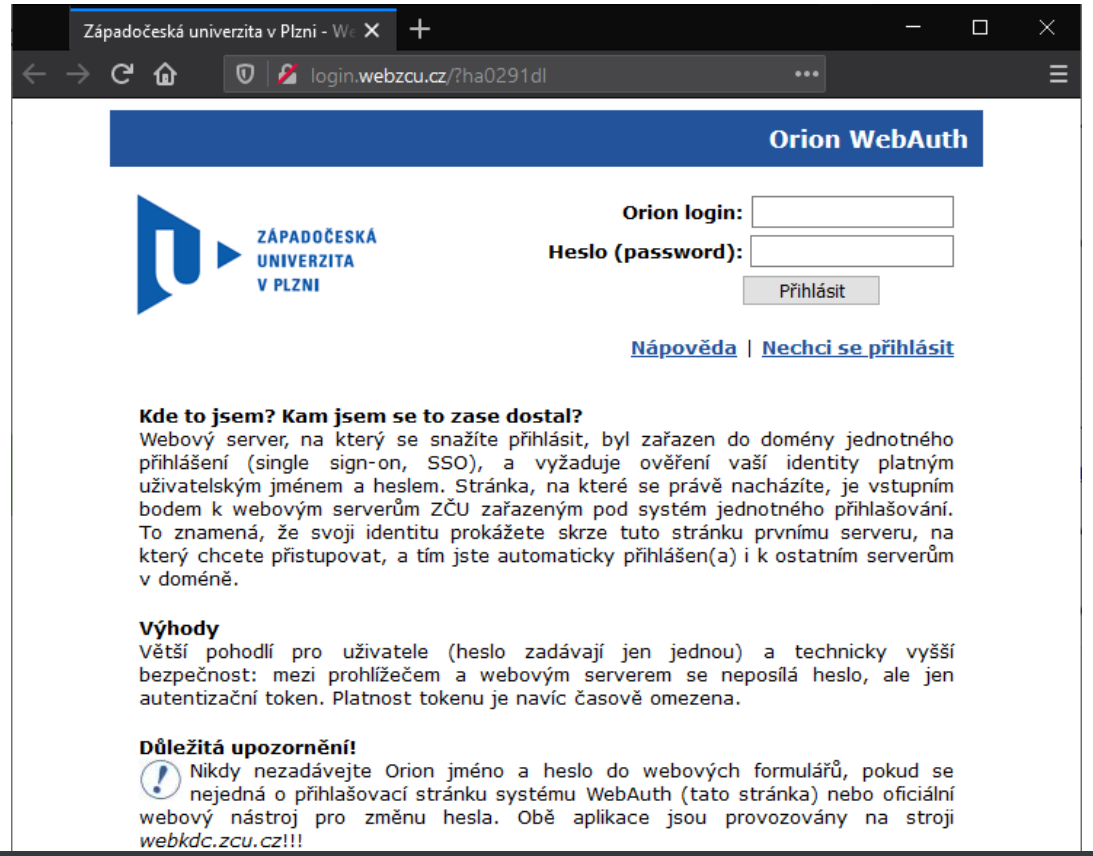
msebela@civ.zcu.cz

Kalendář plánu mezd 2021 je nyní k dispozici:

- http://login.webzcu.cz/?ha0291dl

© Západočeská univerzita v Plzni

Tento e-mail byl zkontrolován programem na viry.



Západočeská univerzita v Plzni - We

login.webzcu.cz/?ha0291dl

Orion WebAuth

ZÁPADOČESKÁ UNIVERZITA V PLZNI

Orion login:

Heslo (password):

Přihlásit

Nápověda | Nechci se přihlásit

Kde to jsem? Kam jsem se to zase dostal?
Webový server, na který se snažíte přihlásit, byl zařazen do domény jednotného přihlášení (single sign-on, SSO), a vyžaduje ověření vaší identity platným uživatelským jménem a heslem. Stránka, na které se právě nacházíte, je vstupním bodem k webovým serverům ZČU zařazeným pod systém jednotného přihlašování. To znamená, že svoji identitu prokážete skrze tuto stránku prvnímu serveru, na který chcete přistupovat, a tím jste automaticky přihlášen(a) i k ostatním serverům v doméně.

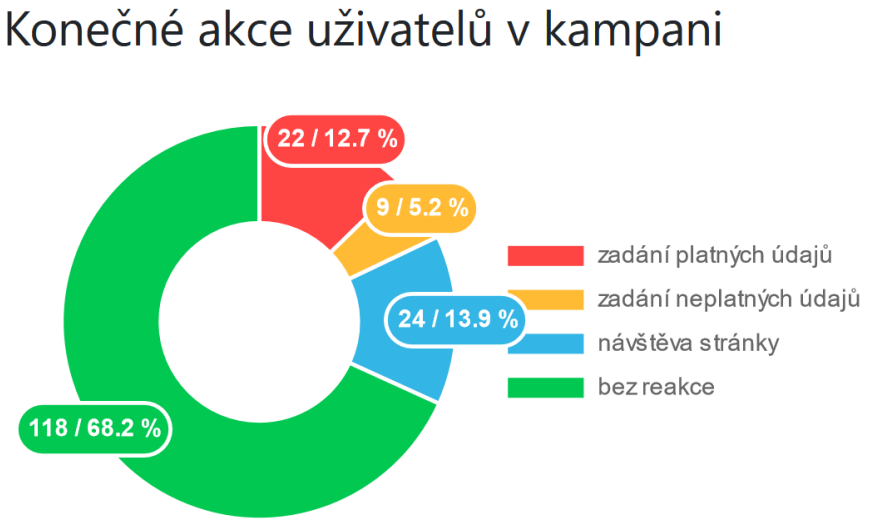
Výhody
Větší pohodlí pro uživatele (heslo zadávají jen jednou) a technicky vyšší bezpečnost: mezi prohlížečem a webovým serverem se neposílá heslo, ale jen autentizační token. Platnost tokenu je navíc časově omezena.

Důležitá upozornění!
Nikdy nezadávejte Orion jméno a heslo do webových formulářů, pokud se nejedná o přihlašovací stránku systému WebAuth (tato stránka) nebo oficiální webový nástroj pro změnu hesla. Obě aplikace jsou provozovány na stroji *webkdc.zcu.cz*!!!

Cvičný phishing (ZČU)

- **Rozesláno 173** vybraným **zaměstnancům**
  - Napříč fakultami a dalšími součástmi ZČU
  - Získáno 22 platných identit během 2 hodin

- **Všechny reakce** příjemců:
  - **Bez reakce (118)**
  - **Návštěva podvodné stránky (24)**
  - Vyplnění **neplatných** přihlašovacích údajů **(9)**
  - Vyplnění **platných** přihlašovacích údajů **(22)**

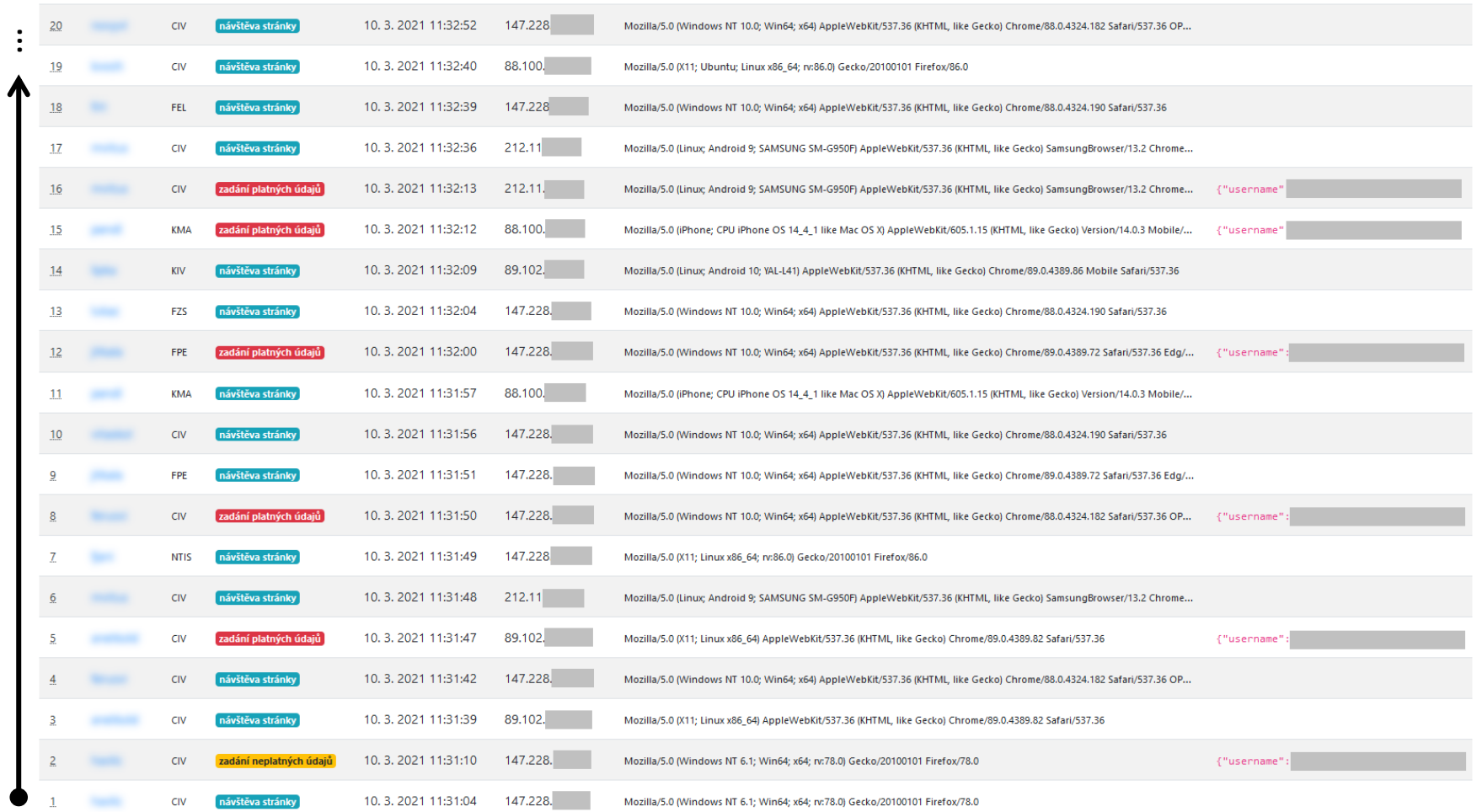


- Realizována stejná kampaň pro dalších **70** zaměstnanců

Časová osa cvičné phishingové kampaně

- **173** odeslaných **e-mailů**

1. **11:30** – odeslání cvičného phishingu
2. **11:31** – první návštěva podvodné stránky
3. **11:31** – první získaná identita
4. **11:35** – získáno 8 platných identit
5. **do 12:00** – získáno 15 platných identit



20	CIV	návštěva stránky	10. 3. 2021 11:32:52	147.228	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36 OP...	
19	CIV	návštěva stránky	10. 3. 2021 11:32:40	88.100.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0	
18	FEL	návštěva stránky	10. 3. 2021 11:32:39	147.228	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36	
17	CIV	návštěva stránky	10. 3. 2021 11:32:36	212.11	Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-G950F) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/13.2 Chrome...	
16	CIV	zadání platných údajů	10. 3. 2021 11:32:13	212.11.	Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-G950F) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/13.2 Chrome...	{"username"
15	KMA	zadání platných údajů	10. 3. 2021 11:32:12	88.100.	Mozilla/5.0 (iPhone; CPU iPhone OS 14_4_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.3 Mobile/...	{"username"
14	KIV	návštěva stránky	10. 3. 2021 11:32:09	89.102.	Mozilla/5.0 (Linux; Android 10; YAL-L41) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.86 Mobile Safari/537.36	
13	FZS	návštěva stránky	10. 3. 2021 11:32:04	147.228.	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36	
12	FPE	zadání platných údajů	10. 3. 2021 11:32:00	147.228.	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.72 Safari/537.36 Edg/...	{"username":
11	KMA	návštěva stránky	10. 3. 2021 11:31:57	88.100.	Mozilla/5.0 (iPhone; CPU iPhone OS 14_4_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.3 Mobile/...	
10	CIV	návštěva stránky	10. 3. 2021 11:31:56	147.228.	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36	
9	FPE	návštěva stránky	10. 3. 2021 11:31:51	147.228.	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.72 Safari/537.36 Edg/...	
8	CIV	zadání platných údajů	10. 3. 2021 11:31:50	147.228.	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36 OP...	{"username":
7	NTIS	návštěva stránky	10. 3. 2021 11:31:49	147.228	Mozilla/5.0 (X11; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0	
6	CIV	návštěva stránky	10. 3. 2021 11:31:48	212.11	Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-G950F) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/13.2 Chrome...	
5	CIV	zadání platných údajů	10. 3. 2021 11:31:47	89.102.	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.82 Safari/537.36	{"username":
4	CIV	návštěva stránky	10. 3. 2021 11:31:42	147.228.	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36 OP...	
3	CIV	návštěva stránky	10. 3. 2021 11:31:39	89.102.	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.82 Safari/537.36	
2	CIV	zadání neplatných údajů	10. 3. 2021 11:31:10	147.228.	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0	{"username":
1	CIV	návštěva stránky	10. 3. 2021 11:31:04	147.228.	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0	

Phishingator

- Systém pro rozesílání cvičných phishingových zpráv

A nechtěl bys jednou za čas poslat cvičný phishing? Abys nezapomněl…

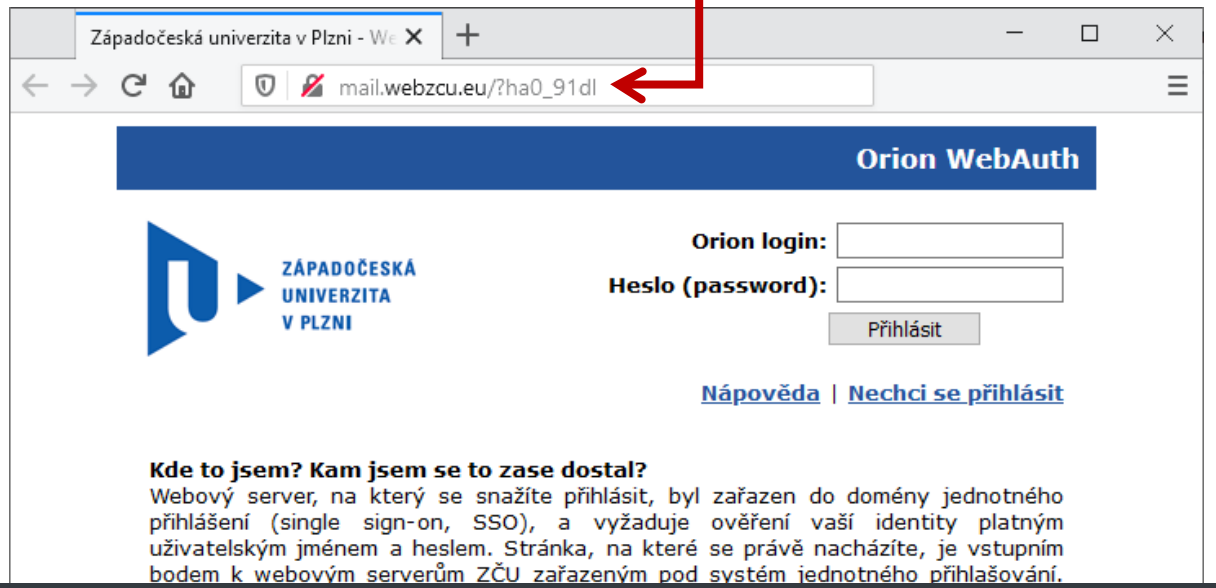
Radši ten cvičný než ten skutečný!

Závěr

- Pozor na typické triky a hlavně na to, kam vedou **odkazy**
  - **„Neklikat automaticky“**
- Útočníci jsou vždy o krok napřed
- Phishing je nejčastější událost v kybernetické bezpečnosti

- **Phishingator**
  - Phishing nanečisto
  - https://phishingator.zcu.cz

Podvodná stránka, která se snaží napodobit přihlášení na ZČU, ale adresa je mail.webzcu.eu (jediná správná je zcu.cz).



ZÁPADOČESKÁ
UNIVERZITA
V PLZNI

Dotazy

Ing. Martin Šebela
msebela@civ.zcu.cz, UI 402

WIRT (*WEBnet Incident Response Team*)
CIV ZČU