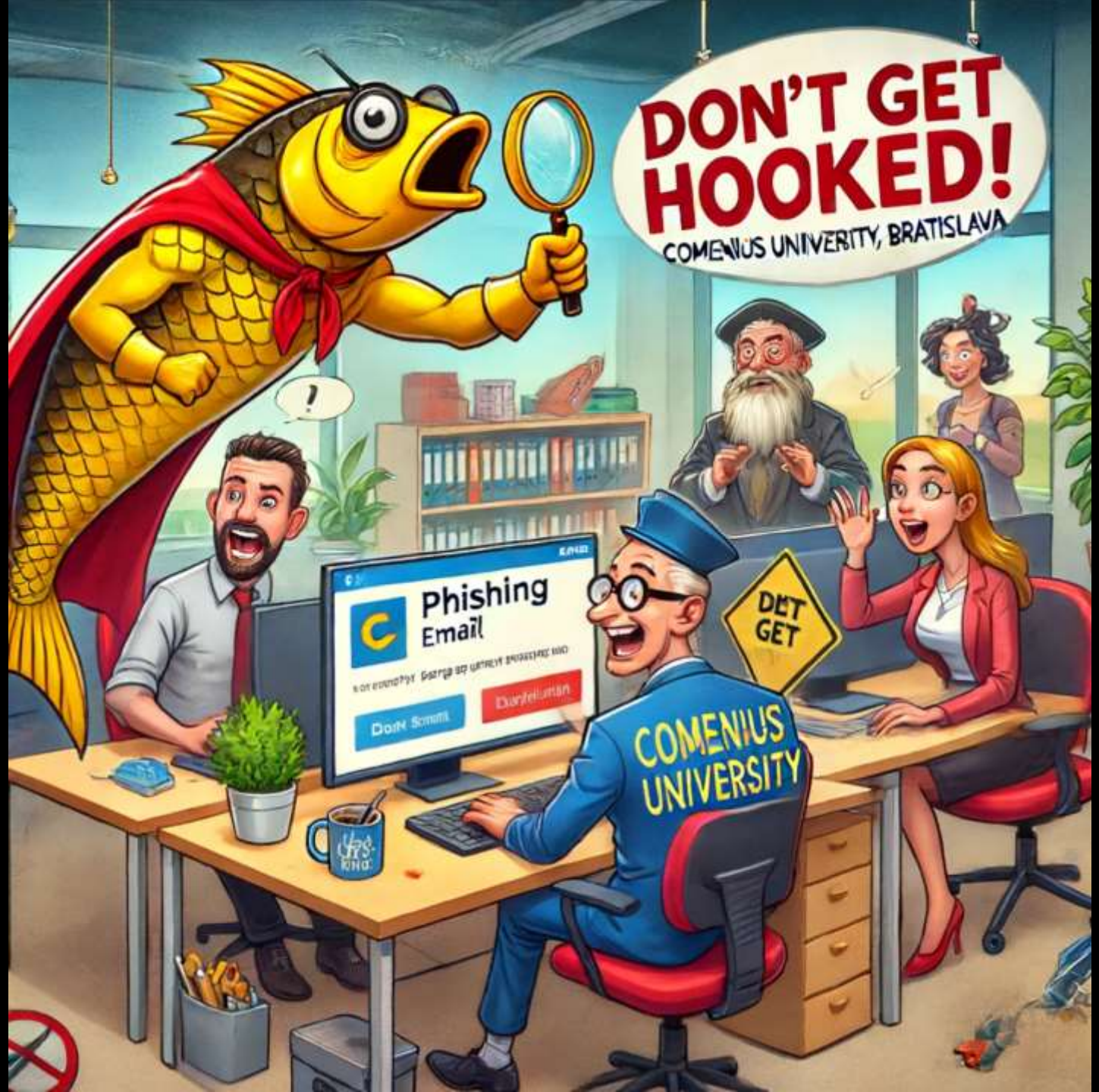
CENTRUM INFORMAČNÝCH TECHNOLÓGIÍ
Univerzita Komenského v Bratislave

# Interný phishingový útok na zamestnancov UK v Bratislave

Beňo Pavel, Štrba Tomáš, Lenhart Michal


DON'T GET HOOKED!
COMENIUS UNIVERSITY, BRATISLAVA
Phishing Email
DET GET
COMENIUS UNIVERSITY

# Čo sme urobili (DIY)

- externý hosting frontend (doména officearena.sk)
- backend na UK
- Vygenerované personalizované linky:
  - zaznamenával sa: klik, email, heslo len áno/nie;
  - výnimky v O365
  - email z aktuálnej karantény O365 - čo najviac znakov phishingu

# Timelime útoku

- Začiatok v nedeľu 15.10.2023 o 19:00
  - postupné posielanie do 23:00

- Informovanie Technických správcov: ráno 16.10. - prečo až ráno ?

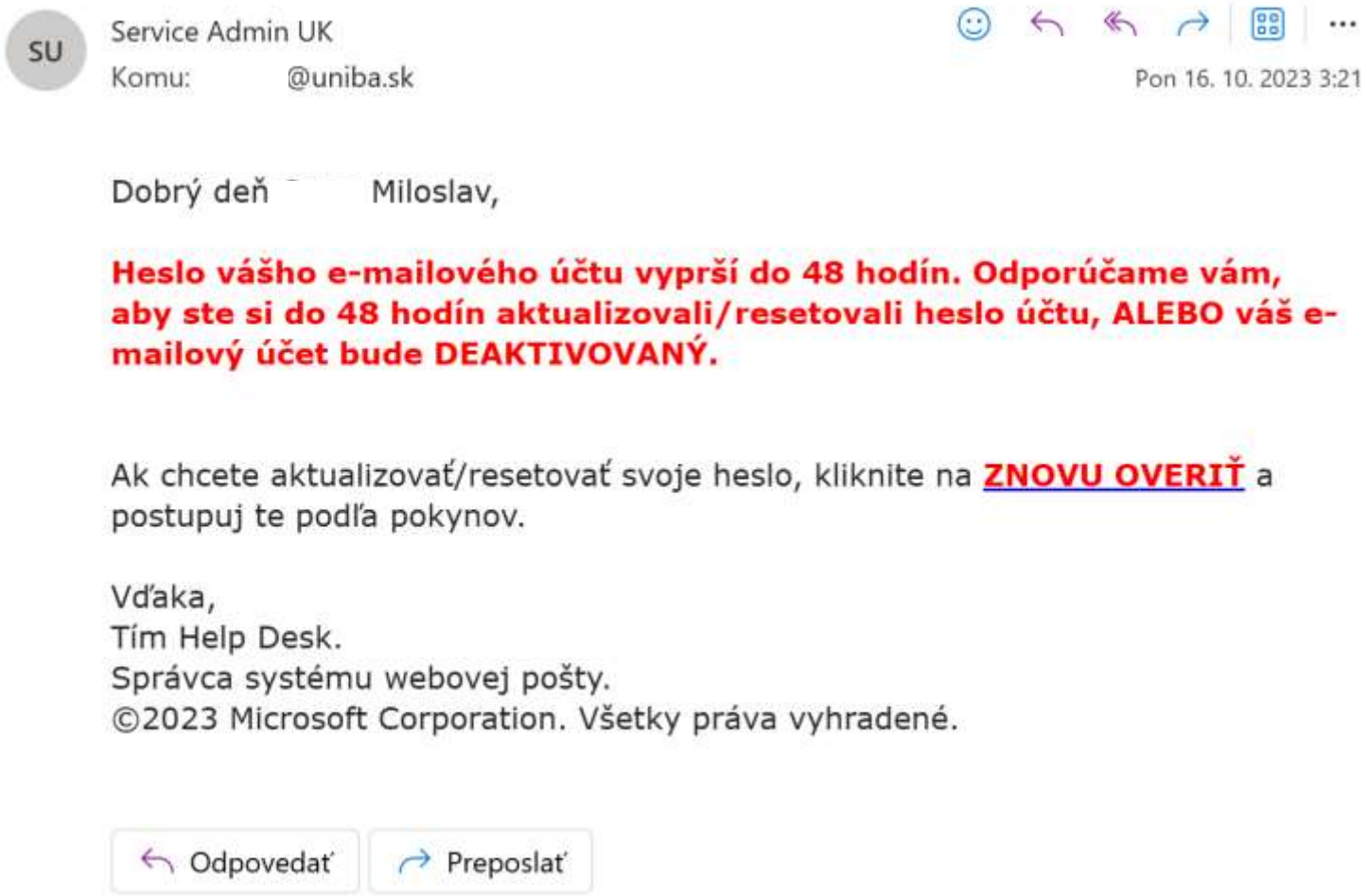
# Generovanie emailu

- Zoznam v sharepoint list naplnený z vygenerovaných linkov:
  - meno
  - priezvisko
  - CDOlogin (univerzitný login)
  - personalizovaný link

- Ukážka linku:
  **https://www.officearena.sk/sign-in/microsoft/user-account/?client_id=bwBwAHAAYQAxAA==**

- Posielanie postupne cez PowerAutomate 19:00 až 23:30

# Phisingový email



SU

Service Admin UK

Komu: @uniba.sk

Pon 16. 10. 2023 3:21

Dobrý deň Miloslav,

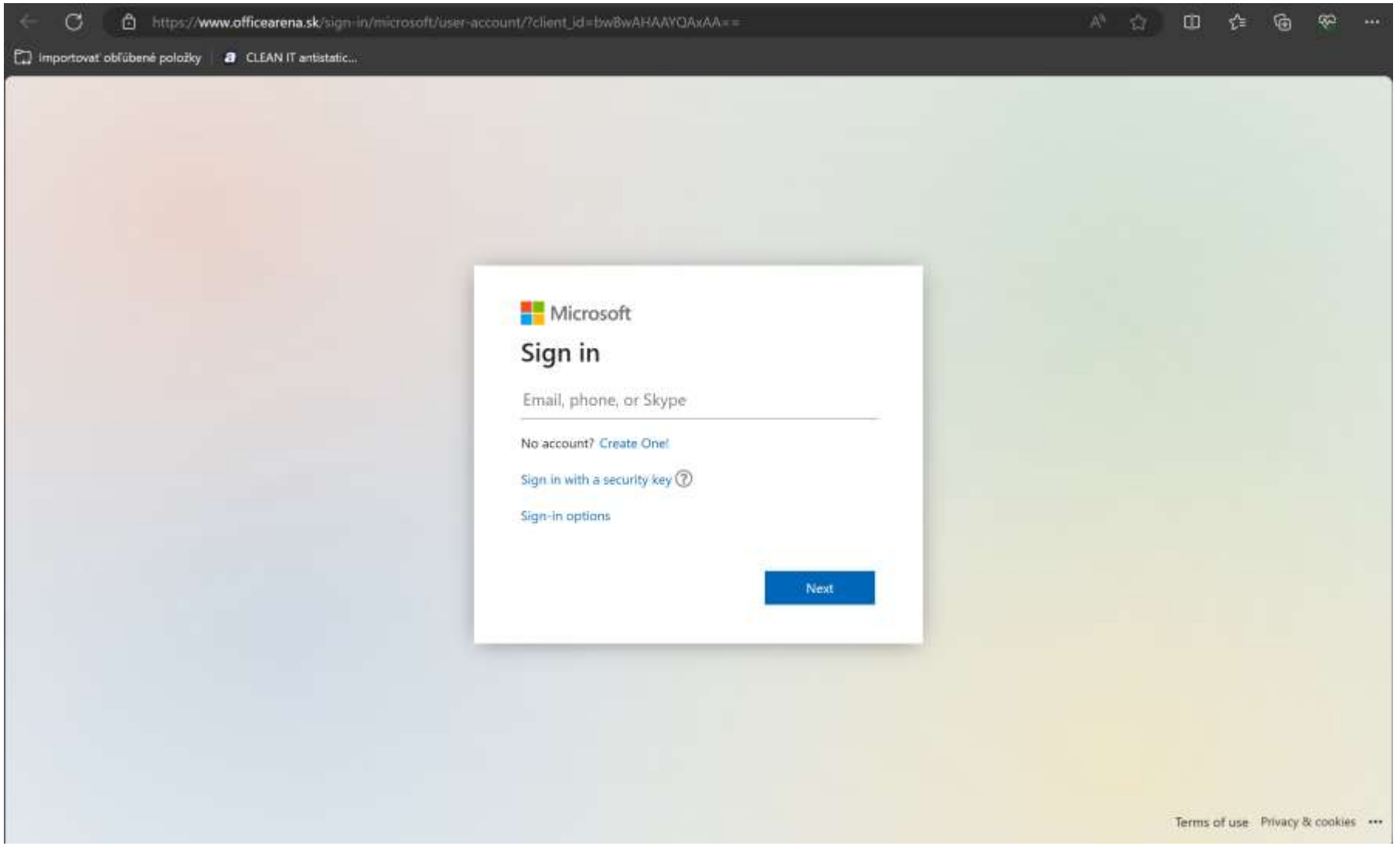
**Heslo vášho e-mailového účtu vyprší do 48 hodín. Odporúčame vám, aby ste si do 48 hodín aktualizovali/resetovali heslo účtu, ALEBO váš e-mailový účet bude DEAKTIVOVANÝ.**

Ak chcete aktualizovať/resetovať svoje heslo, kliknite na **ZNOVU OVERIŤ** a postupuj te podľa pokynov.

Vďaka,
Tím Help Desk.
Správca systému webovej pošty.
©2023 Microsoft Corporation. Všetky práva vyhradené.

Odpovedať Preposlať

# FrontEnd


https://www.officearena.sk/sign-in/microsoft/user-account/?client_id=bwBwAHAAYQAxAA==
Importovať obľúbené položky
CLEAN IT antistatic...
Microsoft
Sign in
Email, phone, or Skype
No account? Create One!
Sign in with a security key
Sign-in options
Next
Terms of use
Privacy & cookies

# BackEnd

- vlastná app, ktorá spracovávala kliknutia na link, resp. vyplnenie údajov
- nezaznamenávali sme heslo ak ho zadali, iba info o zadaní hesla

# Reakcie používateľov

- mail odoslaný cca 5000 zamestnancom (vrátane dohodárov)
- Reakcie:
  - 15.10.2023 (nedeľa po 19:00) -> 80
  - 16. 10.2023 -> 800
  - 17.10.2023 -> 140
  - 18.10.2023 -> 30
- Odovzdané heslá 250 (odovzdaných)/180 (unikátnych cdo loginov)
- Klik na link 660 klikov/360 unikátnych používateľov

- Zaujímavosť: cca 800 používateľov si mail neprečítalo ani po 2 týždňoch ;-)

# Čo s „vinníkmi“?

- každý kto klikol alebo vyplnil dostal email:
  - Ak iba klikol – upozornenie a doporučenie absolvovať školenie KB
  - Ak vyplnil – upozornenie a príkaz na absolvovanie školenia KB

# V čom nám to pomohlo

- presvedčiť vedenie UK a fakúlt o potrebe vzdelávania v oblasti KB pre zamestnancov
- vstupné dáta pred spustením elearningového školenia


- naštartovať aj súčasti v tejto oblasti

# Poučenia z krízového vývoja

- kopec práce aj pre nás (CIT UK), aj pre IT oddelenia na súčastiach (po spustení útoku sa naštartovala lavína
- napriek tomu to stálo za to
- zamestnanci UK čítajú emaily aj v noci (prvá reakcia do pár minút)
- reakcia technických správcov (a IT na súčastiach) veľmi rýchla
- Do 3-4h niektoré webové prehliadače blokovali stránku (preventívne stopnite hyperaktívnych IT zamestnancov)
- nahlasovanie emailov hneď večer
- vtipné emailové adresy v zaznamenaných dátach

CENTRUM INFORMAČNÝCH TECHNOLÓGIÍ
Univerzita Komenského v Bratislave

# Priestor pre vaše otázky

CENTRUM INFORMAČNÝCH TECHNOLÓGIÍ
Univerzita Komenského v Bratislave

# Ďakujem za pozornosť