ENJOY SAFER TECHNOLOGY™

Zaujímavosti z ESET VirusLabu

Ondrej Kubovič, Špecialista na digitálnu bezpečnosť

- Príklady sociálneho inžinierstva
- Útoky cez mail
- Útoky v mobile
- Čo dokážu dnešní útočníci?

Sextortion

Pred nejakým časom som si **zakúpil prístup k e-mailovým účtom od hackerov**. Očividne sa mi ľahko podarilo prihlásiť k vášmu e-mailovému účtu ...

O týždeň neskôr som **nainštaloval Trojan vírus** do operačných systémov všetkých zariadení, ktoré používate pre prístup k vášmu emailu a k ich ovládačom (napr. k vášmu mikrofónu, videokamere a klávesnici).

Stiahol som si všetky vaše informácie, údaje, fotky, históriu prehľadávania webu, mám prístup k vašim aplikáciám, e-mailom, a zoznamu kontaktov.

Skutočne milujete navštevovať **porno stránky** a pozerať vzrušujúce videá. **Nahral som si ich aj vás**...

Ak máte pochybnosti, môžem urobiť pár klikov myšou a všetky vaše videá **budú zdieľané** s vašimi priateľmi, kolegami a príbuznými. Nemám problém ich aj **zverejniť**.

Poďme to vyriešiť: Prepošlete mi **1450e** v bitcoinoch a ja **vymažem** všetky obscénnosti aj škodlivý kód z vašich zariadení. Potom na seba môžeme zabudnúť.

Toto je férová ponuka a cena je celkom nízka vzhľadom na to, že som nejaký čas až doteraz kontroloval váš profil a prenos dát.

Tu je moja bitcoinová peňaženka: 1LsTK4…UvATjfz

Máte menej ako **48 hodín** odkedy ste otvorili tento email. Neodpovedajte mi, žiadna polícia, nehľadajte ma, nesnažte sa preinštalovať zariadenia.

Nemusíte sa obávať, že by som nevedel prijať vaše prevody, že by som si prevod nevšimol, že by som zdieľal vaše videá. **Som predsa férový!**

Moja rada – pravidelne meňte všetky vaše heslá!

Ako sa brániť?

Nahlásiť a následne odstrániť

Používať bezpečnostné riešenie

Tech support scam

Volajú vám z technickej podpory?

Microsoft

Volajú vám z technickej podpory?

- Nevyžiadané
- Zahraničné ale aj slovenské čísla
- V angličtine (najčastejšie indický prízvuk)
- Vydávajú za technickú podporu Microsoftu
- Tvrdia, že vaše zariadenie niekto hackol
- Vedú vás k nastaveniam, ktorým nerozumiete
- Snažia sa získať vzdialený prístup a vaše citlivé či prístupové údaje

Čo s nimi?

- Položiť telefón
- Ak volajú na firemné číslo, nahlásiť IT oddeleniu
- Neposkytovať v telefonáte osobné ani iné údaje

Ak som naletel?

- Čím skôr zmeniť heslá
- Nasadiť dvojfaktorovú autentifikáciu
- Odinštalovať aplikácie podvodníkov
- Kontaktovať banku prípadne iné služby
- Kontaktovať políciu a úrady (SK-CERT)
- Preskenovať zariadenie bezpečnostným softvérom

Škodlivý obsah v mailoch

Problémy s debetnou kartou?

-------- Original message --------
From: SLSP <info@slsp-slovenska.xyz>
Date: 22/04/2021 19:17 (GMT+01:00)
To: [redacted]
Subject: vaša banková karta bola pozastavená

EXTERNAL

SLOVENSKÀ
sporiteľňa

Vašu debetnú kartu sme nateraz pozastavili!

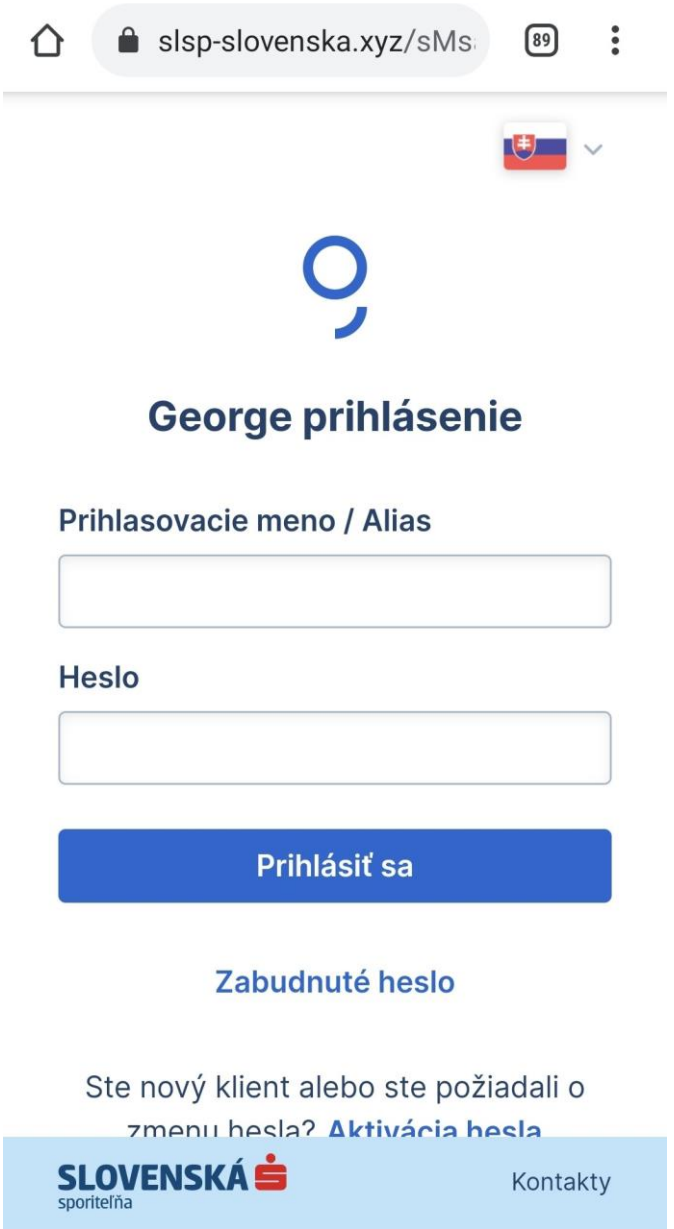
Online platby a výbery hotovosti nemožno uskutočniť, kým sa tento problém nevyrieši.
Potvrďte svoje podrobnosti do nasledujúcich 72 hodín.

Aktivujte moju kartu

Ak máte ďalšie otázky alebo nás chcete kontaktovať, odpovedzte na tento e-mail.

Unsubscribe [redacted]
Update Profile | Customer Contact Data Notice
Sent by info@slsp-slovenska.xyz powered by

Constant Contact
Try email marketing for free today!



Dokumenty na Google Drive?

Wed 11/20/2019 7:58 AM

OG

Olga Geišbergová <olga.solvakia@gmail.com>

Fwd: dokumenty

To

You forwarded this message on 11/20/2019 8:28 AM.

scan_29974.pdf
1 MB

Stiahnuť

Dobré popoludnie
V pokračovaní rozhovoru posielam balík dokumentov.
Na odoslanie potrebujete súhlas.
Celý súbor dokumentov si môžete stiahnuť tu: https://drive.google.com/file/d/1-2X3uQIofDcsVqOFni-MFxvOnhJ/view?usp=sharing
Žiadam o odpoveď najneskôr do 12.11.19

S pozdravom,
Špecialista právneho oddelenia
Olga Geišbergová

ESET ENJOY SAFER TECHNOLOGY™

Nečakané zásielky?

Fwd: Potvrďte svoje náklady na doručenie !

Reply | Reply All | Forward | ...

Tue 1/12/2021 2:18 PM

Od: Slovenská pošta <postmaster@mailer2.savba.sk>
Dátum: 12. januára 2021, 14:15:30 SEČ
[redacted]
Predmet: Potvrďte svoje náklady na doručenie !

Slovenská POŠTA

Ahoj

Posledná pripomienka: Tento e-mail vás informuje, že vaša zásielka stále čaká.

Vaše balenie nebolo možné doručiť **12.01.2021**, pretože nebolo zaplatené žiadne clo **(3,54 EUR)**

Obchodník: Slovenská pošta
Číslo objednávky: 00275029
Suma nákupu: (3,54 EUR)
Dodanie je plánované medzi: 12.01.2021 - 30.01.2021

• Pre potvrdenie odoslania zásielky kliknite sem.

Po príchode na adresu bydliska dostanete e-mail alebo SMS. Na vyzdvihnutie balíka budete mať 8 dní od dátumu dostupnosti. Po výbere budete požiadaní o ID.

• Ak chcete získať viac služieb, kliknutím na tu nájdete ďalšie informácie o vašej zásielke.

Ďakujem za dôveru,

S pozdravom
Váš zákaznícky servis Slovenská pošta.

eset

Online Tracking System

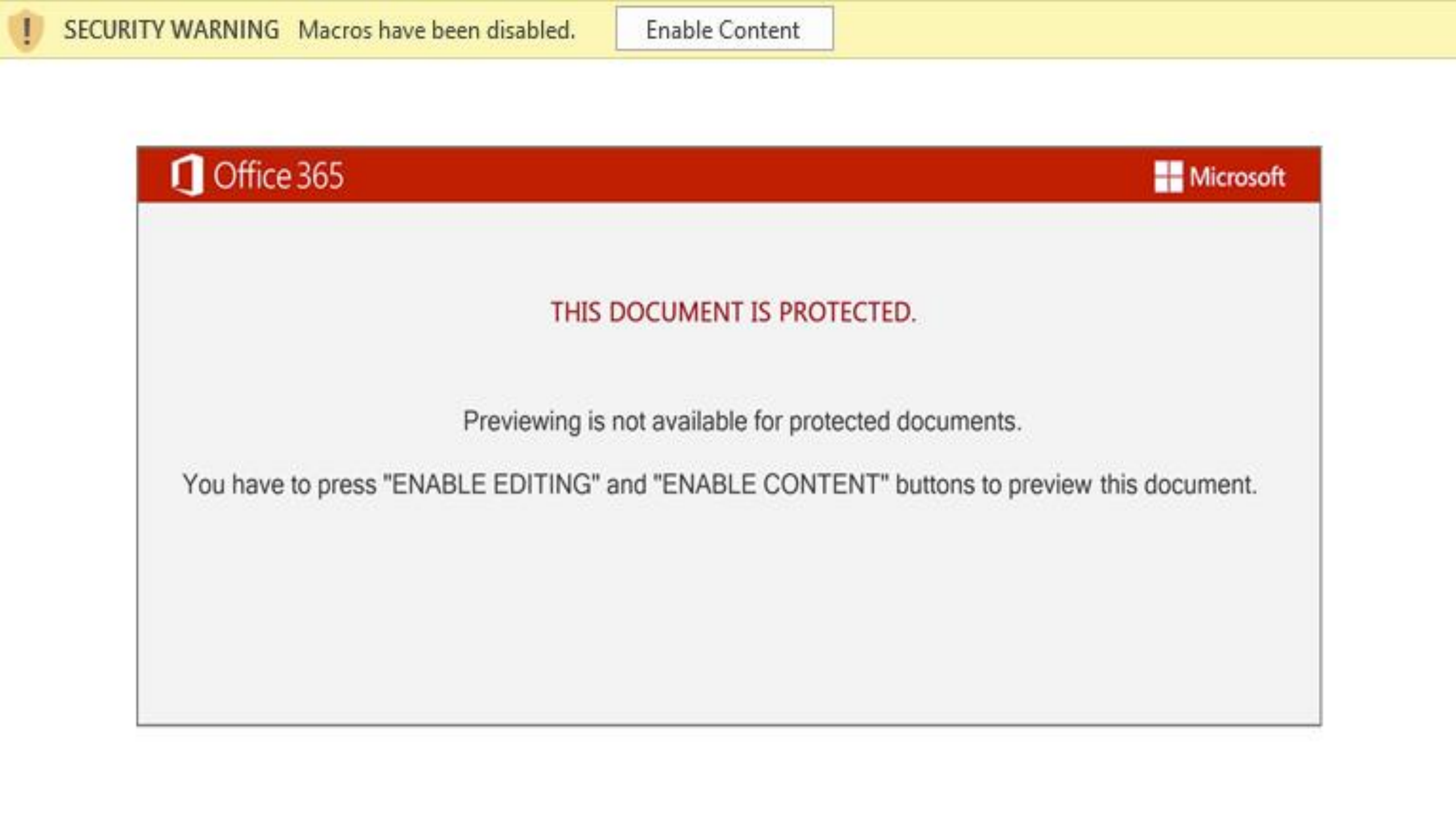
Track Package

Login your E-mail to view package tracking information

.co.nz

Enter Password

Login To View

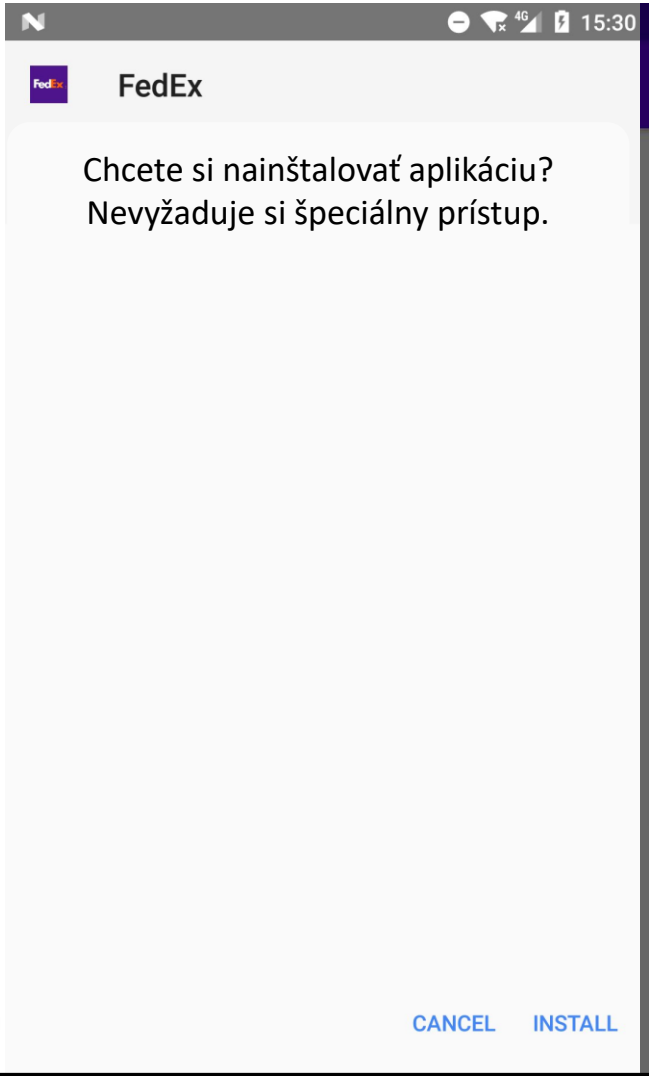

SECURITY WARNING Macros have been disabled.
Enable Content
Office 365
Microsoft
THIS DOCUMENT IS PROTECTED.
Previewing is not available for protected documents.
You have to press "ENABLE EDITING" and "ENABLE CONTENT" buttons to preview this document.

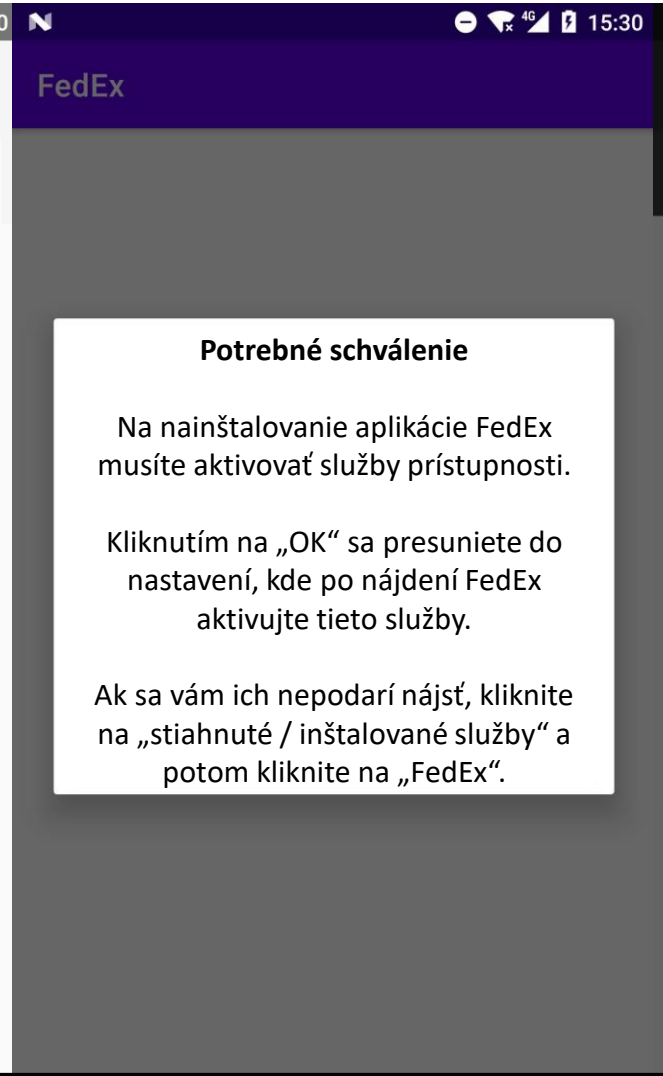
Ako sa brániť?

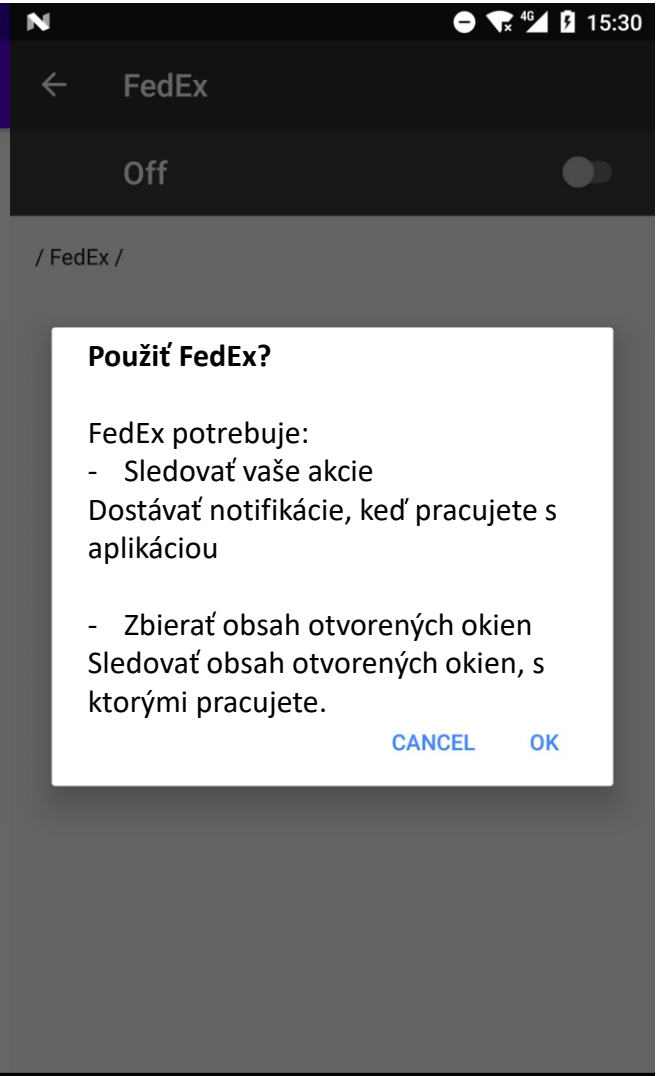
- Mazať podozrivé a nevyžiadané e-maily a správy
- Neotvárať neznáme prílohy
- Neklikať na „enable macros/enable content“
- Nezadávať citlivé údaje na stránkach s podozrivou URL adresou
- Používať viacvrstvový bezpečnostný softvér

Android a zneužívanie služieb prístupnosti

Bankový malvér (FluBot)







Kto všetko zneužíva služby prístupnosti?

- Bankový malware (FluBot, Cerberus, Alien...)
  - Na obchádzanie dvojfaktorovej autentifikácie
- Stalkerware
  - Na sledovanie písaného aj prijatého textu, ale aj špehovanie aplikácií sociálnych sietí a messengerov
- Spyware
  - Na sledovanie písaného aj prijatého textu, ale aj špehovanie aplikácií sociálnych sietí a messengerov

Ako sa brániť?

- Pozor na podozrivé SMS/správy na messengeri
- Nesťahovať appky mimo Google Play
- Čítať recenzie
- Používať bezpečnostný softvér
- Vždy aktualizovať appky aj operačný systém

Je to všetko?

Ani zďaleka...

- Hádať desiatky miliónov hesiel denne
- Šifrovať a kradnúť citlivé dáta
- Otvárať si zadné vrátka
- Útočiť na kritickú infraštruktúru
- Kyberšpionáž a kybersabotáž

Čo s tým?

Vlastná bezpečnosť

- Používajte bezpečné zariadenia
- Používajte bezpečné siete
- Inštalujte si aktualizácie operačných systémov
- Inštalujte si aktualizácie všetkých aplikácií
- Používajte silné heslá
- Používajte viacfaktorovú autentifikáciu
- Vzdelávajte sa

Spoľahlivý bezpečnostný softvér

- Má viacero vrstiev
- Má dobré výsledky v nezávislých porovnaniach
- Má vlastný výskum
- Stará sa o svoj softvér a odstraňuje zraniteľnosti
- Chráni váš počítač, mobilné aj smart zariadenia
- Neobjavil zázračnú technológiu, ktorá vás dokáže 100% ochrániť

100.000.000 používateľov

30 rokov

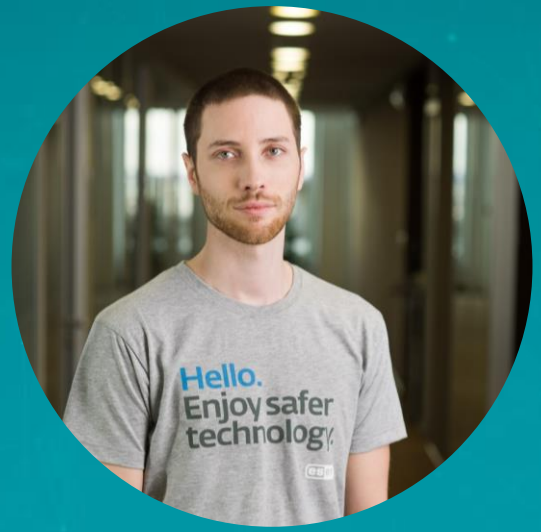
23 pobočiek

13 výskumných centier

chráni

Chrom
e

ENJOY SAFER TECHNOLOGY™



Ondrej Kubovič

Špecialista na digitálnu bezpečnosť

www.eset.com | www.welivesecurity.com