// Obsahuje-li tento dokument zmínky produktů, nejedná se o affiliate program, ale doporučení na základě nezávislých testů a zkušeností.

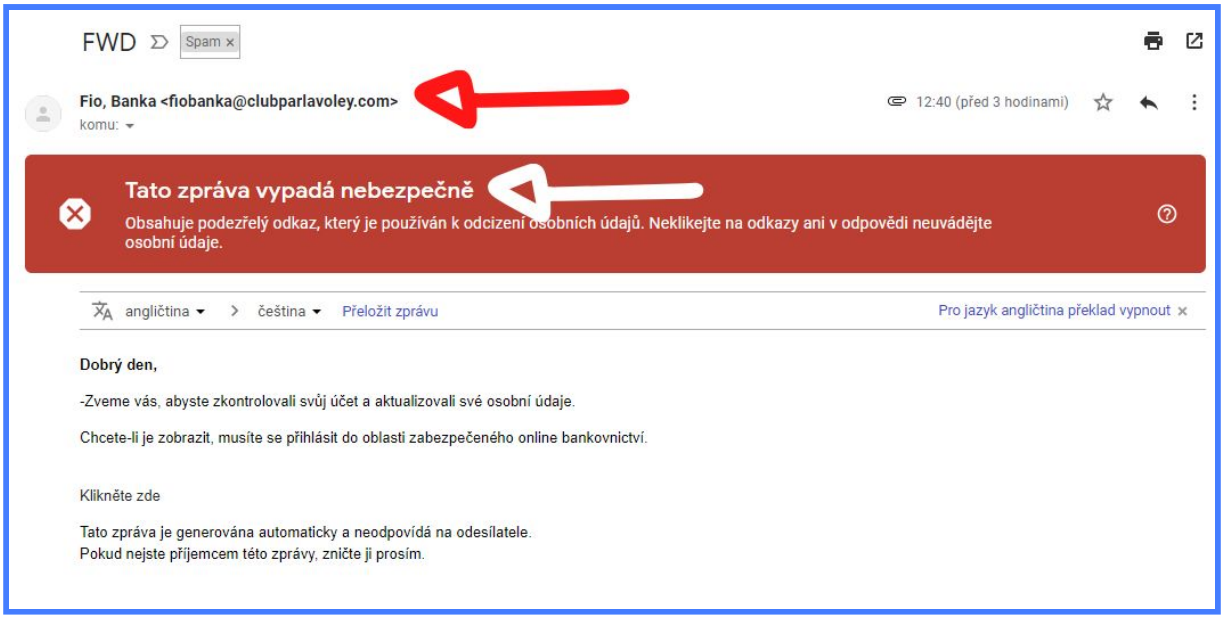
// Chybí vám nějaké informace? Potřebujete radu? Neváhejte mne kontaktovat na webu www.karolsuchanek.com

NAUČTE SE ROZPOZNAT ON-LINE PODVODY

Phishingové e-maily

Pokud vám přišel e-mail od neznámého adresáta, zaměřte se na následující parametry, které mohou poukazovat na pokus o podvod:

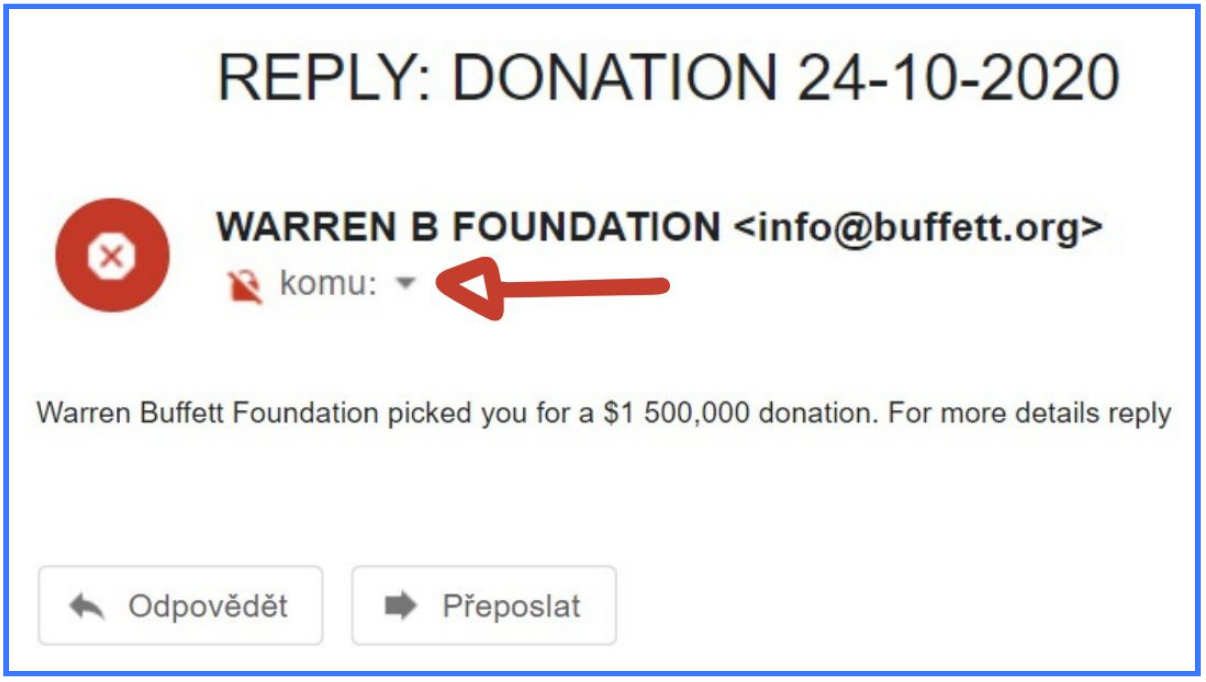
- V podvodných e-mailech velmi často neodpovídá e-mailová adresa jménu odesílatele.
- Příjemci bývají skryti.



- Podvodné e-maily bývají často odeslány v nepravděpodobný čas, například pozdě v noci nebo velmi brzy ráno.

- Předmět zprávy často nijak neodpovídá tématům, o kterých s údajným odesílatelem běžně komunikujete. Stejně tak se může velmi lišit úvodní pozdrav, rozloučení a styl psaní textu.

- Phishingový e-mail je často formulován jako urgentní a požaduje rychlou reakci. Buď s negativním motivem: "Klikněte na link, jinak bude váš účet do 24 hodin smazán!", nebo s příslibem nepravděpodobné odměny, výhry či například dědictví.



- Stále častější je také vydírání, kdy odesílatel tvrdí adresátovi, že má záznamy z jeho webkamery, na kterých je vidět v intimní situaci. Požaduje za smazání záznamů výkupné, ale nelze ověřit, zda takové záznamy skutečně má.

- Často jde o výzvu k zaplacení nějaké objednávky, kterou jste nikdy neudělali, nabídku zboží za nereálně nízkou cenu, žádost o úhradu nesmyslné faktury nebo upozornění na neexistující exekuci.

- Časté jsou pravopisné chyby, nebo je text očividně špatně strojově přeložený z jiného jazyka.

- Podvodné odkazy ve phishingových e-mailech často vypadají na první pohled jako vám známé stránky, ale liší se v nějakém detailu. Například je vynecháno jedno písmeno, nebo naopak doplněn nějaký znak navíc, jako tečka nebo pomlčka. Nebo je namísto koncovky, která by správně měla být .com, .cz nebo .sk použito třeba .net nebo .org

- Často požaduje odesílatel sdělení vašich osobních údajů.

- Škodlivé mohou být přílohy ve formě souborů typu .pif, .scr, .exe nebo .vbs. Závadné soubory také mohou být součástí .zip archivů a škodlivá makra mohou obsahovat také textové dokumenty .docx

TIP: Stránka www.virustotal.com nabízí možnost kontroly jakéhokoliv souboru, či stránky nebo odkazu.

Mohlo by se dle uvedených parametrů jednat o podvodný e-mail? Pokud si nejste nezávadností e-mailu 100% jistí, neotvírejte žádné odkazy ani přílohy!

Pokud znáte člověka uvedeného jako odesílatel, kontaktujte jej telefonicky a ověřte si, zda vám e-mail skutečně odeslal.

Pokud neodeslal (nebo je vám odesílatel neznámý), označte zprávu jako spam. Ve většině mailových služeb se tato volba zobrazí po kliknutí na zprávu pravým tlačítkem myši. Následně zprávu smažte.

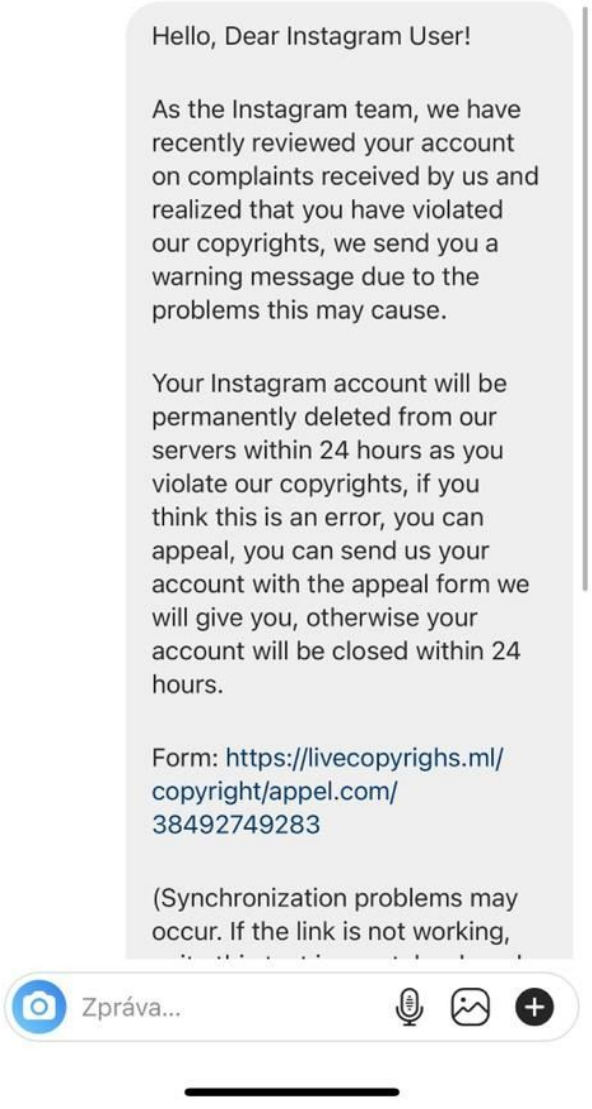
Phishingové zprávy v chatovacích aplikacích

Stále běžnější jsou podvodné zprávy, které mezi sebou lidé dál přeposílají v aplikacích jako Messenger, WhatsApp, Viber, Instagram a další. Může se jednat také o klasickou SMS zprávu.

Často tyto zprávy vyzývají k otevření odkazu a zadání osobních údajů pod záminkou:

- Získání něčeho zdarma - například nákupních poukazů

- Zapojení do soutěže o výhry nepravděpodobně vysoké hodnoty
- Registrace do nějakého systému, například na testy na COVID-19
- Zaplacení objednávky, kterou jste nikdy neprovedli, případně dopravného
- Ověření přihlašovacích údajů například do internetového bankovnictví
- Vyřešení neexistujícího problému s porušením autorských práv na Instagramu: Zpráva upozorňuje, že profil bude do 24 hodin smazán, pokud uživatel neklikne na link pro ověření. Následuje formulář pro zadání přihlašovacích údajů, které pak hacker použije k přihlášení do účtu. Následně heslo změní a znemožní přístup do účtu jeho majiteli.



Odkazy v těchto podvodných zprávách - stejně jako ve phishingových e-mailech - bývají velmi podobné adresám známých webů, ale liší se v detailech (chybějící písmena nebo znaky navíc).

- http://helpformlive.tk
- https://paypal.com.login.pw
- www.faceb00k.com
- www.tesco.com-tesco.com

Pokud si nejste jisti pravostí takové zprávy, opět si odesílatele ověřte telefonicky.

Podvodná reklama a falešné e-shopy

Podvodná reklama na internetu může mít mnoho podob. Často láká na:

- Nepravděpodobně výhodné nabídky e-shopů - zboží za příliš nízké ceny nebo s různými "dárky" navíc
- Podvodné on-line soutěže o atraktivní ceny, ve kterých je snadné vyhrát a následně je vyžadováno zadání osobních údajů
- Nepravděpodobně výhodné investice
- Nabídky něčeho zdarma, například nákupních poukazů

Podvodné on-line reklamy často vedou na falešné e-shopy, které mohou napodobovat známé e-shopy. Vždy si zkontrolujte správnost odkazu! Pokud jste narazili na nabídku e-shopu, který ještě neznáte, zkontrolujte si kontaktní údaje.

Seriózní e-shop jasně uvádí veškeré zákonné údaje (obchodní jméno, IČO, DIČ, bankovní spojení, telefon, adresu fyzickou i elektronickou, odpovědné osoby, pracovní dobu), které jsou ověřitelné v obchodním rejstříku, tedy třeba na www.justice.cz nebo www.orsr.sk.

Podezřelé bývají hlavně příliš levné e-shopy, které umožňují pouze platbu předem. Chcete-li někde nakoupit poprvé, volte vždy dobírku, neplaťte předem! Vhodné je také vyhledat si obchod na některém ze serverů, které se zabývají jejich recenzemi a hodnocením, třeba Heureka.

TIP: Proti rizikům online podvodů je možné se pojistit. Pojišťovny většinou nabízejí produkt pod názvem *pojištění kybernetických rizik*.