DOXO LOGIC

7 ČASTÝCH PASTÍ HACKERŮ

na které se zaměstnanci nechávají nachytat

Zpracováno společností DoxoLogic, s.r.o.

Až 96 % všech hackerských útoků je vedeno přes e-mail.

Pro internetové útočníky je nejjednodušší cestou, jak se dostat na vaše data a systémy, váš zaměstnanec.

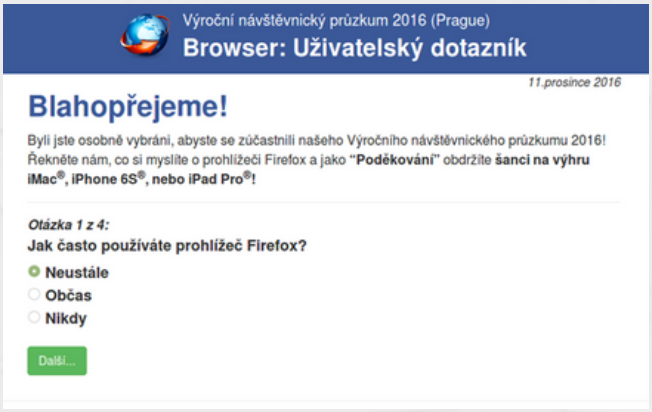
Zmanipulovat zaměstnance k otevření e-mailu a následnému kliknutí na nebezpečný odkaz není vůbec složité. Falešné e-maily jsou dnes už opravdu propracované a na první pohled nelze úplně odhalit, že se jedná o podvod.

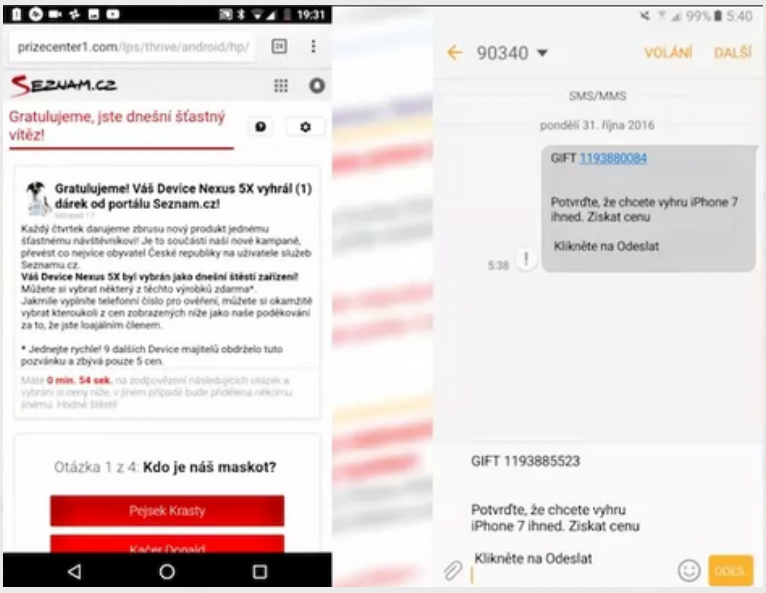
Na co se nejčastěji vaši zaměstnanci nechají nachytat?

1 VÝHRY A SOUTĚŽE

Každý rád vyhrává. A právě na to sází internetoví útočníci. Díky lákavé výhře často lidé bezmyšlenkovitě klikají na vše, jen aby vyhráli.

Velmi často jsou ve falešných výhrách produkty značky Apple. Nejnovější iPhone vám skutečně nikdo zadarmo nedá!





Zpracováno společností DoxoLogic, s.r.o.
+420 601 526 886 www.doxologic.cz info@doxologic.cz

NAŠE RADA

"Červená kontrolka" by se každému měla rozblikat, pokud pro vyzvednutí výhry musí zadávat údaje své platební karty.

2 FALEŠNÉ FAKTURY A DOKUMENTY

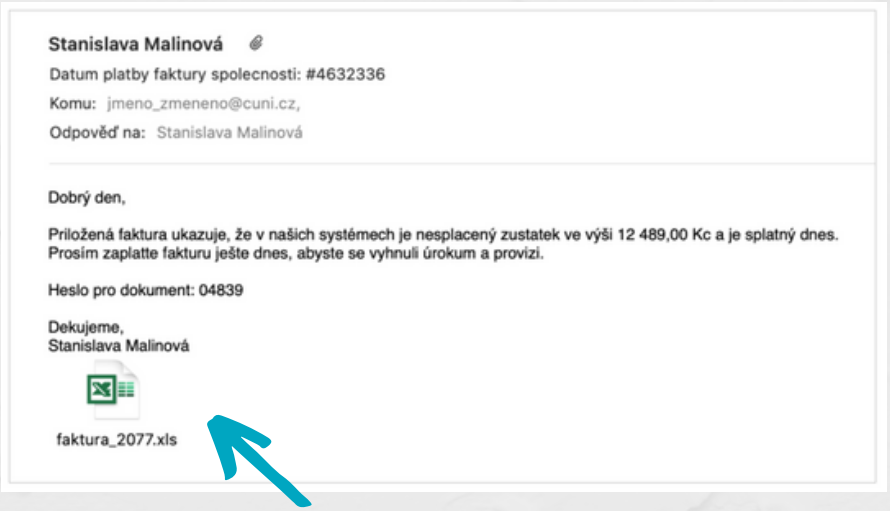
Nachytat zaměstnance na otevření falešné faktury je snadné. Lidé nepřemýšlí, proč faktura přišla právě jim, když nejsou účetní a s fakturami nemají nic společného.

Velmi dobře zde funguje lidská zvědavost. A na to hackeři sází.

Stejné je to i u dalších dokumentů. E-maily vypadají věrohodně, dokonce i patička e-mailu odpovídá skutečné společnosti.

NAŠE RADA

E-maily od neznámých odesílatelů, které obsahují přílohu a požadují její otevření, raději ignorujte.
Pečlivě si také prohlédněte celý e-mail, především adresu, ze které přišel a patičku e-mailu.


Stanislava Malinová

Datum platby faktury spolecnosti: #4632336

Komu: jmeno_zmeneno@cuni.cz,

Odpověď na: Stanislava Malinová

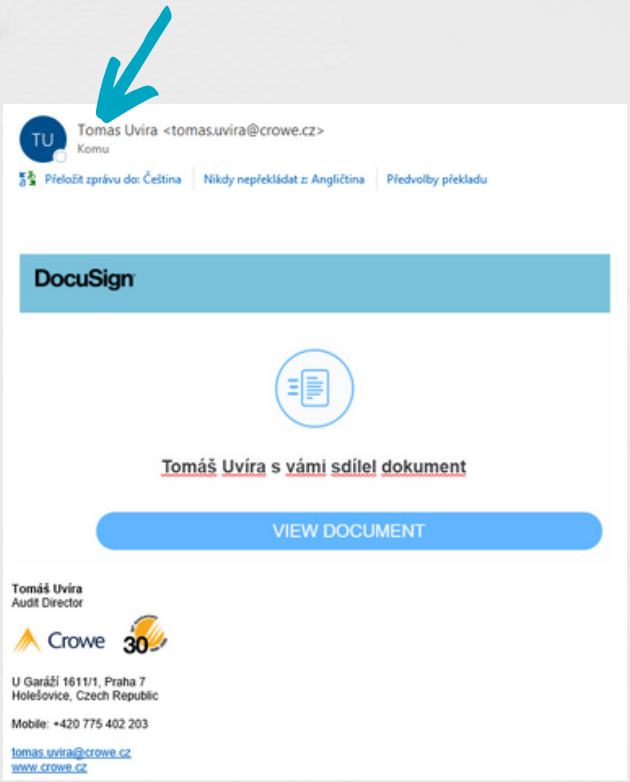
Dobrý den,

Priložená faktura ukazuje, že v našich systémech je nesplacený zustatek ve výši 12 489,00 Kc a je splatný dnes. Prosím zaplatte fakturu ješte dnes, abyste se vyhnuli úrokum a provizi.

Heslo pro dokument: 04839

Dekujeme,
Stanislava Malinová

faktura_2077.xls

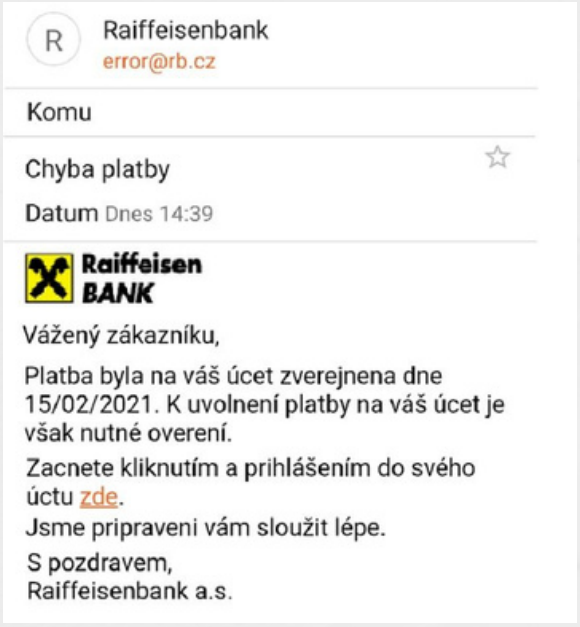


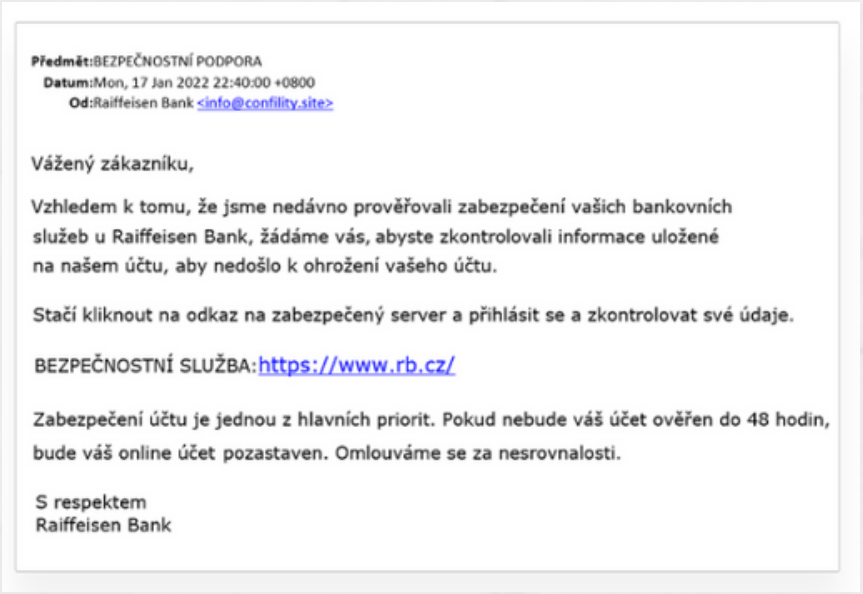
3 ZPRÁVY Z BANKY

Falešné e-maily z bank jsou velmi věrohodné. Často obsahují logo banky, podpis a kontaktní údaje. Díky tomu je e-mail ještě důvěryhodnější.

Útočníci vyzývají k ověření identity nebo účtu pod hrozbou jeho zablokování. Opět je zde využita technika nátlaku a naléhavosti.

Pozor také na falešné SMS zprávy!





Předmět:BEZPEČNOSTNÍ PODPORA
Datum: Mon, 17 Jan 2022 22:40:00 +0800
Od: Raiffeisen Bank <info@confility.site>

Vážený zákazníku,

Vzhledem k tomu, že jsme nedávno prověřovali zabezpečení vašich bankovních služeb u Raiffeisen Bank, žádáme vás, abyste zkontrolovali informace uložené na našem účtu, aby nedošlo k ohrožení vašeho účtu.

Stačí kliknout na odkaz na zabezpečený server a přihlásit se a zkontrolovat své údaje.

BEZPEČNOSTNÍ SLUŽBA:https://www.rb.cz/

Zabezpečení účtu je jednou z hlavních priorit. Pokud nebude váš účet ověřen do 48 hodin, bude váš online účet pozastaven. Omlouváme se za nesrovnalosti.

S respektem
Raiffeisen Bank

NAŠE RADA

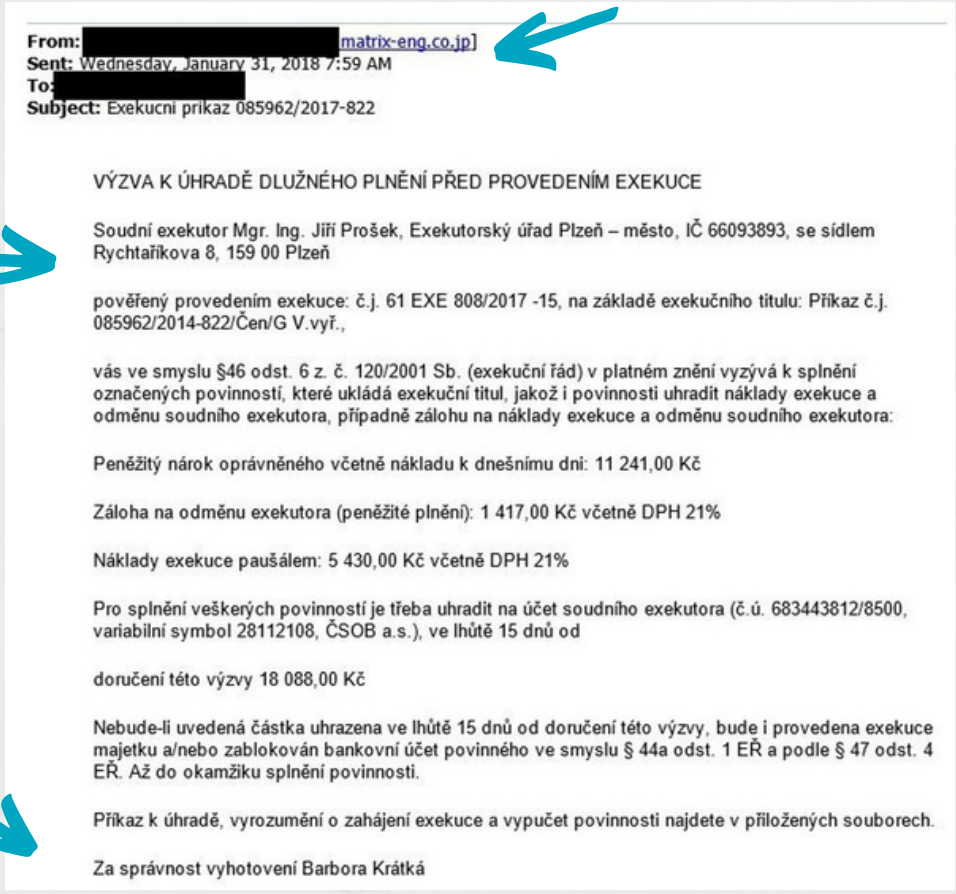
- Mějte se na pozoru vždy, když e-mail působí **naléhavě nebo výstražně** a **vyžaduje po vás neobvyklou aktivitu**.
- Banky ve svých e-mailech **nikdy neodkazují přímo na stránku internetového bankovnictví.** Pro vstup na váš účet vždy zadejte adresu banky do adresního řádku prohlížeče.
- Pokud se stanete obětí útoku, ihned kontaktujte vaši banku pro zablokování účtu.

4 EXEKUČNÍ PŘÍKAZY

Podvodné zprávy se tváří jako soudní příkaz k uhrazení dluhu a vyhrožují exekucí. Při otevření zavirují počítač.

Hackeři zde využívají pocit strachu. I když si člověk není vědom žádného dluhu, přesto se chce přesvědčit a na odkaz klikne.

Často z medií slýcháme případy, kdy lidé netušili, že dluží na pokutě za MHD, dokud nepřišla exekuce. Proto se také není čemu divit a hackeři to moc dobře vědí!



From: [redacted]matrix-eng.co.jp]
Sent: Wednesday, January 31, 2018 7:59 AM
To: [redacted]
Subject: Exekucni prikaz 085962/2017-822

VÝZVA K ÚHRADĚ DLUŽNÉHO PLNĚNÍ PŘED PROVEDENÍM EXEKUCE

Soudní exekutor Mgr. Ing. Jiří Prošek, Exekutorský úřad Plzeň – město, IČ 66093893, se sídlem Rychtářikova 8, 159 00 Plzeň

pověřený provedením exekuce: č.j. 61 EXE 808/2017 -15, na základě exekučního titulu: Příkaz č.j. 085962/2014-822/Čen/G V.vyř.,

vás ve smyslu §46 odst. 6 z. č. 120/2001 Sb. (exekuční řád) v platném znění vyzývá k splnění označených povinností, které ukládá exekuční titul, jakož i povinnosti uhradit náklady exekuce a odměnu soudního exekutora, případně zálohu na náklady exekuce a odměnu soudního exekutora:

Peněžitý nárok oprávněného včetně nákladu k dnešnímu dni: 11 241,00 Kč

Záloha na odměnu exekutora (peněžité plnění): 1 417,00 Kč včetně DPH 21%

Náklady exekuce paušálem: 5 430,00 Kč včetně DPH 21%

Pro splnění veškerých povinností je třeba uhradit na účet soudního exekutora (č.ú. 683443812/8500, variabilní symbol 28112108, ČSOB a.s.), ve lhůtě 15 dnů od

doručení této výzvy 18 088,00 Kč

Nebude-li uvedená částka uhrazena ve lhůtě 15 dnů od doručení této výzvy, bude i provedena exekuce majetku a/nebo zablokován bankovní účet povinného ve smyslu § 44a odst. 1 EŘ a podle § 47 odst. 4 EŘ. Až do okamžiku splnění povinnosti.

Příkaz k úhradě, vyrozumění o zahájení exekuce a vypučet povinnosti najdete v přiložených souborech.

Za správnost vyhotovení Barbora Krátká

NAŠE RADA

- Vždy zkontrolujte e-mail odesílatele. Pokud je z jiné domény než .cz buďte opatrní.
- Pokud e-mail obsahuje kontaktní údaje, nebojte se si zprávu ověřit.
- Dříve než si e-mail ověříte, rozhodně na nic neklikejte a neotevírejte žádné zaslané odkazy.

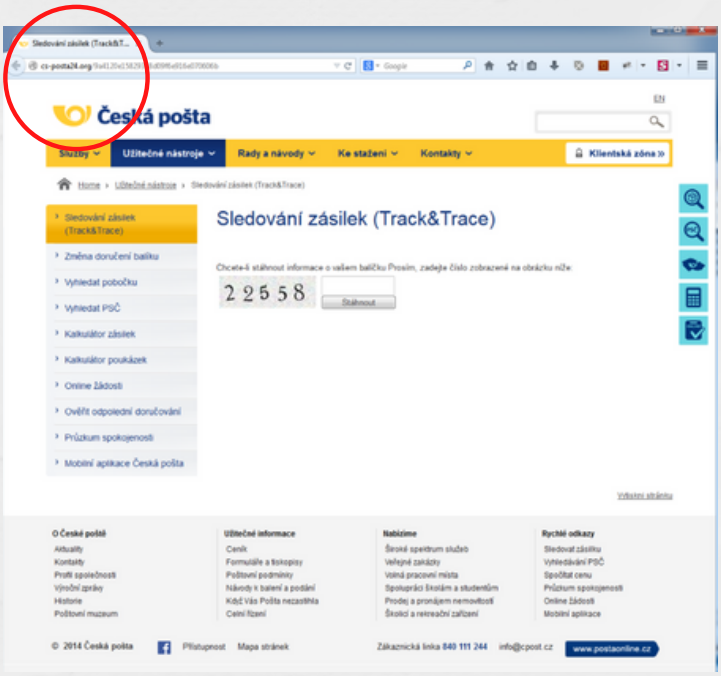
5 SLEDOVÁNÍ ZÁSILKY

Falešné e-mailové zprávy nejčastěji zneužívající společnosti Česká pošta, GLS, atd.

Zpráva obsahuje informaci o možnosti sledování zásilky, která je určena pro vás. Hackeři zde opět sází na vaši zvědavost.

Ukázka útoku

Krok 1: Odkaz v e-mailu vás odvede na stránku, která vypadá úplně stejně jako stránky České pošty. Až na URL adresu (cs-posta24.org). Toho si ale málokdo všimne.



Krok 2: Po zadání kódu pro sledování zásilky jste vyzváni ke stažení souboru.

Krok 3: Po stažení souboru dojde k zašifrování veškerých vašich dat a výzvě k zaplacení za zpřístupnění.

NAŠE RADA

Dříve než otevřete zaslaný odkaz v e-mailu, ověřte si, kam skutečně vede. **To uděláte jednoduše pouhým najetím myši na text odkazu.**

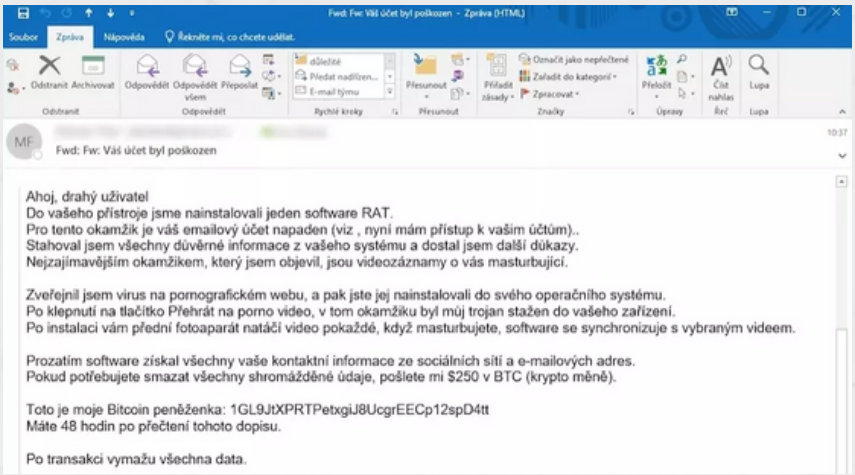
6 VÝHRUŽKY SE ZVEŘEJNĚNÍM CHOULOSTIVÝCH NAHRÁVEK

Podvodné e-maily, ve kterých útočníci údajně natočili oběť při sledování videa pro dospělé a za to, že video nezveřejní mezi jejich kontakty, požadují platbu v Bitcoinech.

Útočníci tvrdí, že v počítači je vir, který umožňuje sledovat dění uživatele a připojit se k jeho webkameře. Často ani lidem nedojte, že webkameru na svém zařízení nemají a výkupné zaplatí.

NAŠE RADA

Pokud po vás chce neznámý odesílatel platbu v Bitcoinech, ve většině případů se jedná o podvod!
E-mail vymažte ze své mailové schránky a na nic neklikejte.



7 ZADÁNÍ PŘIHLAŠOVACÍCH ÚDAJŮ

Jedná se o falešné e-mailové zprávy, které z nás mají vylákat přihlašovací údaje k našim účtům (e-mail, bankovní účet, atd.)

Po kliknutí na zaslaný odkaz jste přesměrování na webovou stránku, která zdánlivě vypadá stejně, jako např. web vaší banky.

Protože většina lidí používá jedno stejné heslo k více účtům, je pak pro internetového útočníka jednoduché, dostat se i na firemní systémy a aplikace.

----- Original Message -----
From: Česká spořitelna
To:
Sent: Tuesday, December 02, 2014 7:33 AM
Subject: Naléhavý Naléhavé od Česká spořitelna II

ČESKÁ SPOŘITELNA

Aktualizace Aktivace účtu Česká spořitelna

Vážený zákazniku

Chtěli bychom zdůraznit, že přístup do vašeho internetového bankovnictví je brzy skončí. Aby bylo možné i nadále využívat on-line bankovnictví, žádáme vás o potvrzení své údaje pomocí odkazu níže.

Aktualizujte svůj on-line bankovní účet: klikněte zde

Budeme automaticky obnovovat on-line bankovní účet, a budete kontaktování jedním z našich zaměstnanců. Internetové bankovnictví umožňuje rychlý a snadný přístup k vašemu účtu. Můžete snadno převést peníze pomocí jediného kliknutí.

Vážený uživateli,

Velmi se vám omlouváme, ale došlo k bezpečnostním problémům a z toho důvodu je nutné, aby nám na adresu nicpodpora@secmail.pro každý uživatel který má registrovaný email s doménou zaslal tyto udaje uzivazelské jmeno, heslo abychom mohli ověřit, že je to skutečně onen uživatel
a ne zločinec, ktery narušil náš bezpečnostní systém.
---
na adresu nicpodpora@secmail.pro zašlete e-mail ve tvaru:

name:"uzivazelske jmeno"
passwd:"heslo"

Tedy např.:
name:"podpora@secmail"
passwd:"radio"

Děkujeme za pochopení.

S pozdravem
podpora CZ.NIC, správce domény CZ

NAŠE RADA

- Nikdy nezadávejte své přihlašovací údaje na výzvy zaslané e-mailem.
- Vždy si prověřte e-mail odesílatele.
- Pro každý svůj účet používejte různé heslo. Abyste si je nemuseli pamatovat, využijte správce hesel např. passspack.com, který je zdarma.