
## V aktuálním IT Kompasu jsme pro Vás připravili:

**108. číslo**

Vybrané aktuality ze světa IT
Tipy – Triky
Soutěž
Vtip pro dobrou náladu

## Vybíráme zajímavé aktuality:

**Odborníci na kybernetickou bezpečnost odhalili zranitelnosti chytrých aut**
Vedle masivních útoků je možné napadnout propojené automobily prostřednictvím řady jednoduchých technik. Více...

**Nové způsoby vykrádání peněz z našich bankovních účtů**
Názvem "BackSwap" byl označen malware, který používá zcela nové metody vykrádání peněz z bankovních účtů obětí. Více...

Více aktualit naleznete na www.AntiviroveCentrum.cz nebo na Facebooku .

## Tipy a triky

## Jak na dovolené ochránit svůj bankovní účet, fotky a zařízení?

Podle Eurostatu pocestuje na zahraniční dovolenou přibližně každý pátý obyvatel Česka. I během ní chtějí mít cestovatelé a dovolenkáři přístup k internetu, v jejich zavazadlech tak pocestují i mobily, tablety a jiná technika. Společnost ESET i my doporučujeme tyto kroky:

**PŘED DOVOLENOU**

- Aktualizujte operační systém a všechny programy na zařízeních, které berete s sebou na dovolenou. Na mobil si nainstalujte aplikaci pro internetové bankovnictví od vaší banky, aplikace oblíbených sociálních sítí, e-mailu a také aplikace obchodů, pokud víte, že na nich budete chtít během dovolené nakupovat.
- Zvažte instalaci bezpečnostní aplikace, která dokáže při ztrátě nebo krádeži lokalizovat na dálku telefon a nebo vymazat jeho obsah. Jde například o aplikaci ESET Mobile Security .
- Na mobilu a laptopu si nastavte automatické uzamykání na PIN nebo otisk prstu, které se spustí po krátké době nečinnosti.
- Zálohujte si obsah zařízení, která si berete na dovolenou.
- V bance anebo na jejím webu se informujte, jakým způsobem byste měli z dovolené nahlásit jakýkoli potenciální problém s vaším účtem, ať už by šlo o neznámou transakci nebo ztrátu platební karty. Soustřeďte se především na telefonní číslo, protože banky mají obvykle pro telefonické hovory se zahraničím vyčleněnou speciální linku.
- Na webu se informujte, před jakými internetovými podvody v dané zemi varují jiní dovolenkáři a cestovatelé.

**BĚHEM DOVOLENÉ**

- Při jakémkoli podezření na neoprávněnou transakci informujte svoji banku.
- Pokud budete používat Wi-Fi sítě, o jejichž bezpečnostním nastavení nic nevíte, používejte internetové prohlížeče jen k běžnému surfování po webech, které nevyžadují žádné přihlašovací údaje a ani jejich prostřednictvím nebudete posílat žádné údaje. Pokud je totiž Wi-Fi napadena nebo někdo sledujte data, která jsou odesílaná přes tuto síť, v podstatě všechno, co přes tyto weby odešlete dál, dokáže odchytit. Přes prohlížeče byste se proto určitě neměli přihlašovat do svého e-mailu, internetového bankovnictví, na sociální sítě, a ani byste neměli nakupovat přes různé e-shopy.
- Pro sledování e-mailu, sociálních sítí, internetového bankovnictví a online nakupování využívejte výhradně originální mobilní aplikace. Tyto aplikace totiž mezi vaším mobilem a serverem těchto služeb komunikují šifrovaně a tudíž bezpečněji.
- V hotelu a kavárně si ověřte, jak se jmenuje jejich oficiální Wi-Fi síť a připojujte se pouze k ní. Útočníci totiž často vytváří falešné sítě s podobným názvem. Pokud Wi-Fi síť podmiňuje vaše připojení k internetu aktualizací softwaru, odpojte se od ní a nepoužívejte ji. Pravděpodobně se někdo pokoušel vaše zařízení infikovat. Používejte Wi-Fi sítě se zabezpečením minimálně na úrovni WPA2. A mobilech s Androidem si úroveň zabezpečení zkontrolujete v nastaveních. V iPhonech vás operační systém sám upozorní na špatně zabezpečenou síť.
- S laptopem je nejbezpečnější surfovat na neznámém Wi-Fi připojení s VPN, tedy virtuální privátní sítí. VPN aplikaci je však třeba nainstalovat dopředu.

## Jak nejlépe poznat phishing?

Na rozdíl od běžných rybářů, které můžete potkat v pohodlných křesílcích na březích řek a rybníků, vysedávají rhybáři u počítačů a líčí pasti na internetové uživatele. Termín rhybář v češtině označuje počítačového hackera, který se snaží obohatit prostřednictvím phishingu – zákeřné techniky, která se někdy do češtiny překládá jako rhybaření. Jejich úlovky tvoří osobní data uživatelů nebo údaje z platebních karet. Bezpečnostní odborníci ze společnosti Kaspersky Lab Vám na následujících řádcích poradí, jak se nechytit na jejich háčky.

1. Přesvědčte se o správnosti odkazu ještě před tím, než na něj kliknete. Najetím kurzoru na uvedený odkaz se vám ukáže URL adresa, kterou si pečlivě přečtěte. Mějte oči na stopkách před pravopisnými chybami, špatným hláskováním a dalšími nesrovnalostmi.
2. Svá uživatelská jména a hesla zadávejte pouze v případě, že je navázáno zabezpečené připojení. To poznáte díky předponě "https" před samotnou adresou internetové stránky. Pokud "s" chybí, mějte se na pozoru.
3. I když Vám přijde zpráva nebo e-mail od kamaráda, mějte na paměti, že se hackeři mohli nabourat do jeho účtu. Proto byste měli být i v takových případech ostražití a dávat si pozor především na zprávy obsahující odkazy nebo podezřelé přílohy.
4. Oznámení z banky, úřadu, e-shopu, cestovní kanceláře nebo od aerolinek se dají velmi jednoduše zfalšovat. Podvodníci Vás jejich prostřednictvím budou často vyzývat k zaplacení účtů či neproběhlých plateb nebo žádat o zaslání Vašich citlivých osobních údajů. Ověřte si nejprve, jestli se nejedná o podvod.
5. Neklikejte na odkazy v e-mailu. Raději si otevřete nové okno v prohlížeči a URL banky či jiné stránky zadejte ručně.
6. Pokud narazíte na phishingovou zprávu, nahlaste ji příslušné bance nebo sociální síti, jejímž jménem zpráva komunikuje. Oznamování podvodů opravdu pomáhá při pronásledování zločinců.
7. Snažte se nepřihlašovat do online bankovnictví, když jste připojeni k veřejné WiFi. Volně dostupné hotspoty jsou v dnešní době velmi praktické, ale pro přihlášení do online bankovnictví raději využijte svá mobilní data nebo počkejte na zabezpečenou síť. Otevřené sítě mohou totiž být vytvořeny speciálně pro účely kyberzločinu a sloužit hackerům jako zdroje cenných dat a vašich financí.
8. Neotevírejte neočekávané soubory, které vám posílají virtuální hráči online her. Mohlo by se jednat o zákeřný ransomware nebo spyware.
9. Nikdy nesdílejte s třetí stranou citlivé údaje, jako jsou přihlašovací údaje a hesla, údaje o platebních kartách apod. Oficiální společnosti nikdy nebudou žádat o tento typ údajů prostřednictvím e-mailu.
10. Využívejte účinné bezpečnostní řešení, které ochrání vaše zařízení a veškerá data v něm uložená. Antivirový software, jako je například Kaspersky Internet Security , vyřeší většinu problémů automaticky a upozorní vás na nebezpečí, pokud to bude nutné. Pamatujte při tom, že efektivní ochranu potřebuje nejen váš pevný počítač, ale i notebook a mobilní zařízení.

## Soutěž

**Vyhodnocení minulé soutěže:**
Na otázku z minulého vydání elektronického magazínu IT Kompas odpověděl správně a z mnoha správných odpovědí byl vylosován pan P.K., kterému tímto gratulujeme k výhře softwaru Norton Security Standard pro 1 PC na rok zdarma.

**Otázka zněla:**
Co označuje v informatice pojem "Tor"?

**Správná odpověď měla být:**

Tor je v informatice názvem softwarového systému zajišťujícímu anonymizaci uživatele při pohybu na Internetu, k čemuž využívá model klient-server. Uživatel využívá klientskou část a jeho datový tok prochází nejprve sítí Tor složené ze serverových částí a teprve pak k cílovému počítači. Tím je možné skrýt informace o IP adrese uživatele a dalších faktorů, které by ho mohly identifikovat. Díky používání Toru je obtížnější vysledovat stopy činnosti uživatele na Internetu včetně návštěv webových stránek, on-line příspěvků, programů pro komunikaci v reálném čase (instant messaging) a dalších forem komunikace. Je určen k ochraně osobních údajů uživatelů, jejich svobody, soukromí, a možnosti provádět důvěrné obchodování, tím že je chrání před sledováním jejich aktivit na Internetu.

Více informací naleznete zde.

**Nová otázka:**

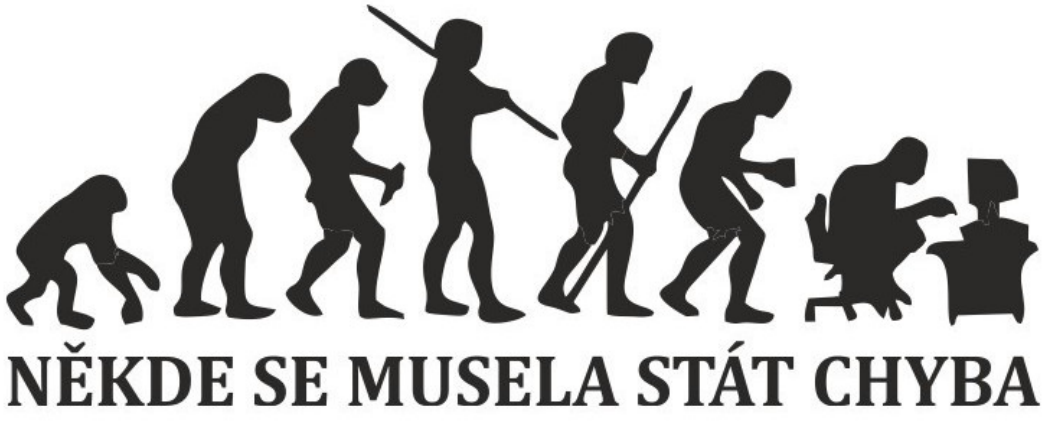
**Co označuje v informatice pojem "Blockchain"?**

Ze správných odpovědí vylosujeme výherce, který od nás získá Sticky Password Premium pro 1 uživatele na rok zdarma.

Odpovědi pište do 20. 7. 2018 na e-mail amenit@amenit.cz .

Správnou odpověď a výherce uveřejníme v příštím čísle. Pokud se chcete co nejdříve dozvědět, zda jste vyhráli, staňte se našimi přáteli na Facebooku. Tam se informace o výherci objeví jako první.

## Vtip pro dobrou náladu



Vydání IT Kompasu od 1. čísla naleznete zde.

**Tým Antivirového Centra**
Amenit s.r.o.

ANTIVIROVÉ CENTRUM - MÁTE SE KAM OBRÁTIT

---

Amenit s.r.o. - jsme s vámi již od roku 1998, tel.: 556 706 203, 222 360 250

Nezobrazuje-li se vám e-mail správně, klikněte prosím zde.