JOSEF JAVORA

TISPARTNERS
TRUSTED INFORMATION SECURITY

10+1 RADA

jak se nestat obětí hackerů!

CO STAČILO VČERA, DNES JIŽ NESTAČÍ

NEMUSÍTE ČÍST CELOU PŘÍRUČKU

– pokud víte, proč se chcete chránit a nepotřebujete inspiraci, můžete rovnou přeskočit do kapitoly:
„Co musím nezbytně mít a jak se mám chovat…“

Doufám ale, že vydržíte – i kdybyste měli jasno, co chcete pořídit pro ochranu, je dobré mít jistotu.
Protože to, co stačilo včera, dnes již nestačí. (O zítřku nemluvě.)

JAK VNÍMÁTE ONLINE RIZIKA?

Pokud čtete tyto řádky, mám dobrý důvod se domnívat, že nějaká online rizika vnímáte. A to je dobře! Dnes se totiž v online světě všichni nejen pohybujeme, ale také jsme sem převedli spoustu našich aktivit: soukromých i pracovních, využíváme mnoho služeb, a hlavně online platíme! Z tohoto virtuálního světa se tak stal rozsáhlý sociální systém. Jakési velkoměsto, které nám přináší na jedné straně plno výhod, pohodlí, informací, příležitostí a možností. Na straně druhé také rizika – jako každé velkoměsto. Protože zloději a vlastně všichni zločinci v tak velkém systému, jakým dnes online svět je, vidí především peníze a také hodně možností, jak skrýt svoje zločinné chování a nechat se chytit.

My, kteří se v tomto městě (nebo džungli?) pohybujeme, se musíme chránit:

- Především vhodným a zodpovědným chováním, abychom někomu nedávali zbytečnou příležitost,
- technickými nástroji, protože by nás mohla ruční ochrana stát všechno úsilí a čas, které potřebujeme na něco jiného.

Nikdy si ale nemůžeme být jisti, jestli jsme pro svoji ochranu udělali skutečně všechno, co je nezbytné. Museli bychom se totiž učit stále. Online svět se totiž vyvíjí velice rychle. Stejně rychle se ale vyvíjejí hackerské nástroje a také chuť zločinců dostat se do naší peněženky.

CHRÁNIT SVOJE PC JE DNES NELEHKÝ ÚKOL

Výrobci PC, operačních systémů a softwaru nám to moc nezjednodušují. Prodávají svoje produkty plné chyb a zranitelností, které pak hackeři zneužívají pro svoje nekalé aktivity.
Dal jsem si za cíl vám na těchto stránkách nabídnout radu a pomoc, která je úplně zadarmo. Budu rád, když ji využijete a když vám pomůže chránit se před nebezpečím, které vám hrozí. Snad vám pomůže i v případě, kdy budete hledat také placené nástroje na ochranu - nejen na našem e-shopu.

Výrobci operačních systémů a softwaru nejsou zrovna nadšení mluvit o tom, kde mají svoje zranitelná místa. *(Důvodem není ani tak jejich obava z toho, že by tyto informace zneužili hackeři: ti to samozřejmě dělají a vědí o těchto zranitelnostech všechno, co potřebují.)* Nezní totiž moc hezky, když si zákazník udělá takový obrázek o tom, co kupuje: *Systém, který se rychle vyvíjí, do kterého se snaží přidávat neustále nové funkce a komfort. S každou novou verzí se do něj zavedou další chyby, zranitelnosti a mezery, které se mohou stát vstupní branou pro hackerský útok. Neustálými záplatami pak dohánějí to, co mělo být bezpečné a funkční už při prodeji – bohužel pro rychlost vývoje nebyl čas na dostatečné testování.*

Za slovo „Systém“ na začátku minulého odstavce si můžete dosadit jméno vašeho oblíbeného operačního systému nebo jiného softwaru, který denně používáte. Možná vás ani nenapadlo, že je plný chyb, které vás mohou ohrozit.

Je to trochu podobné, jako ve světě aut: i tam se nám může stát, že výrobce objeví nějakou chybu, která může být příčinou nehody – takže čas od času musíme do servisu, kam výrobce svolá svoje zákazníky k jejímu odstranění. Ruku na srdce: chtěli byste používat auto, se kterým musíte na „svolávačku“ do servisu každý týden?

Já tedy ne. Bohužel ve světě PC, tabletů a mobilů, softwaru a souvisejících služeb nám nic jiného nezbývá.

Snad i tady jednou dojde na to, že my jako zákazníci vyvineme dostatečný tlak na výrobce, aby více investovali do testování svých aplikací a nezkoušeli to na nás, zákaznících.

Ještě poznámka: Dělám všechno pro to, aby tomuto textu rozuměli všichni – ti, kteří na počítačích, mobilech a dalších zařízeních pracují nebo se baví, ať už jsou pro ně tato zařízení černými skříňkami, kterými se nechtějí moc zabývat, nebo jsou to nadšenci pro informační technologie a snaží se proniknout do problematiky hlouběji. Některým odborným výrazům se ale vyhnout nedá. Když na něco takového narazíte, zadejte si patřičný termín do Wikipedie, kde většinou najdete potřebné vysvětlení.

Nebo si můžete pořídit moji knihu *Informační bezpečnost pro domácí uživatele a malé kanceláře*, kde vše vysvětlím ve zkratce, ale věřím, že dostatečně srozumitelně. Chystám pro vás také videokurz a e-mailový kurz - v případě zájmu sledujte naše stránky.

CO MUSÍM NEZBYTNĚ MÍT A JAK SE MÁM CHOVAT…

10 DOBRÝCH RAD PRO ODPOVĚDNÉ CHOVÁNÍ ONLINE

NEJDŘÍVE, JAK SE CHOVAT

Odpovědné chování je to první, na co se musíme zaměřit. A to platí v oblasti ochrany života, majetku, v dopravě, třeba v džungli a vůbec kdekoliv, kde nám hrozí nějaké nebezpečí. Je dobré si osvojit zásady, díky kterým bude naše bezpečí o mnoho vyšší než bezpečí těch, kteří to neřeší. Pojďme se podívat na pár zásad, které lze označit jako zásady správné hygieny online:

1. Nepoužívej nechráněné WiFi sítě.

V internetové kavárně, na nádraží, v parku – je samozřejmě příjemné mít zdarma připojení k internetu. Pokud jde ale o veřejnou WiFi síť, která není patřičně chráněna, může být takové připojení opravdu nebezpečné. Obzvlášť v případě, kdy během připojení zadáváte kamkoli přístupové nebo platební údaje. Pokud se jejich použití nemůžete vyhnout, určitě si pořiďte solidní VPN (viz samostatný odstavec níže).

2. Chraň si svoje osobní údaje.

Nesvěřujte je nikomu, kdo pro jejich držení nemá dostatečný důvod a komu skutečně nedůvěřujete.

3. Používej dostatečně dlouhá a odolná hesla.

Krátké heslo je možné prolomit za pár sekund, dostatečně dlouhé heslo, které se skládá také z velkých písmen, číslic a dalších znaků, může být dnes prakticky nerozluštitelné. Existuje více webových stránek, kde si můžete ověřit kvalitu vašeho hesla a teoretickou dobu potřebnou na jeho prolomení. Rychle můžeme například zjistit, že heslo „ahoj“ může být rozluštěno za 11 mikrosekund, zatímco heslo „3bra3z2.patra“ (tedy tři bratři z druhého patra) za 33 tisíc let…

4. Nerecykluj svoje přístupové údaje a hesla.

Používejte vždy hesla nová – nikdy je neobměňujte jednoduchým způsobem, jako je třeba číslovka aktuálního roku umístěná na konci. Pokud je zrecyklujete, může se snadno stát, že hacker ukradne databázi hesel z oblíbeného e-shopu a pak zkouší, jestli nebude pasovat i jinde – třeba s nějakou modifikací.

5. Věz, že ostatní uživatelé stejné sítě se mohou stát Tvým ohrožením.

Jakmile se pohybujeme ve společném síťovém prostředí (třeba v domácí síti), je pro nás každé napadnuté/hacknuté zařízení významným rizikem. Nejedná se jen o vaše PC, ale také další zařízení, jako mobily, tablety a další „chytré“ krabičky, které mají vlastní síťové připojení (to dnes může mít i pračka nebo televize). Myslíte-li vaši bezpečnost vážně, je důležité starat se také o to, jak se chovají ostatní uživatelé.

6. Dbej na neustálou aktuálnost svých systémů.

O zranitelnostech systému jsme si řekli výše (vzpomeňte si na svolávačky aut do servisu). Každou aktualizaci je třeba provést co nejdříve. Otálení

vede v lepším případě k opomenutí. Horší je, že zveřejněním aktualizace dá výrobce světu (také hackerům) vědět o chybě/zranitelnosti, které naše zařízení má. A to je bohužel pro hackery snadné vidět i za pomoci legálních nástrojů. Dá se bez nadsázky říci, že říkáme celému světu: „Hele, podívejte se, mám doma nefunkční alarm a zámky taky nepatří k těm nejodolnějším!“. Ideální pozvánka pro zločince.

7. Nepracuj na svém PC s administrátorským oprávněním.

Jde o hodně rozšířený nešvar, kdy máme jako uživatel zároveň zapnuté administrátorské oprávnění. A o velkou chybu, kterou děláme, aniž bychom si uvědomili nebezpečnost takového jednání: ve chvíli, kdy se objeví jakýkoliv virus, či malware, má volné pole působnosti. Často jde o poslední, ale největší bariéru, která mu stojí v cestě. Pokud je to i váš případ, vytvořte si, pokud možno, ihned nového uživatele, kterému přiřadíte administrátorské oprávnění. To pak sobě odeberete. Pokud bych některé z nabízených opatření považoval za nejdůležitější, je to právě tohle. Velmi jednoduchým způsobem posunete svoji bezpečnost o desítky procent!

8. Měj se na pozoru před sociálním inženýrstvím, phishingem a spamy.

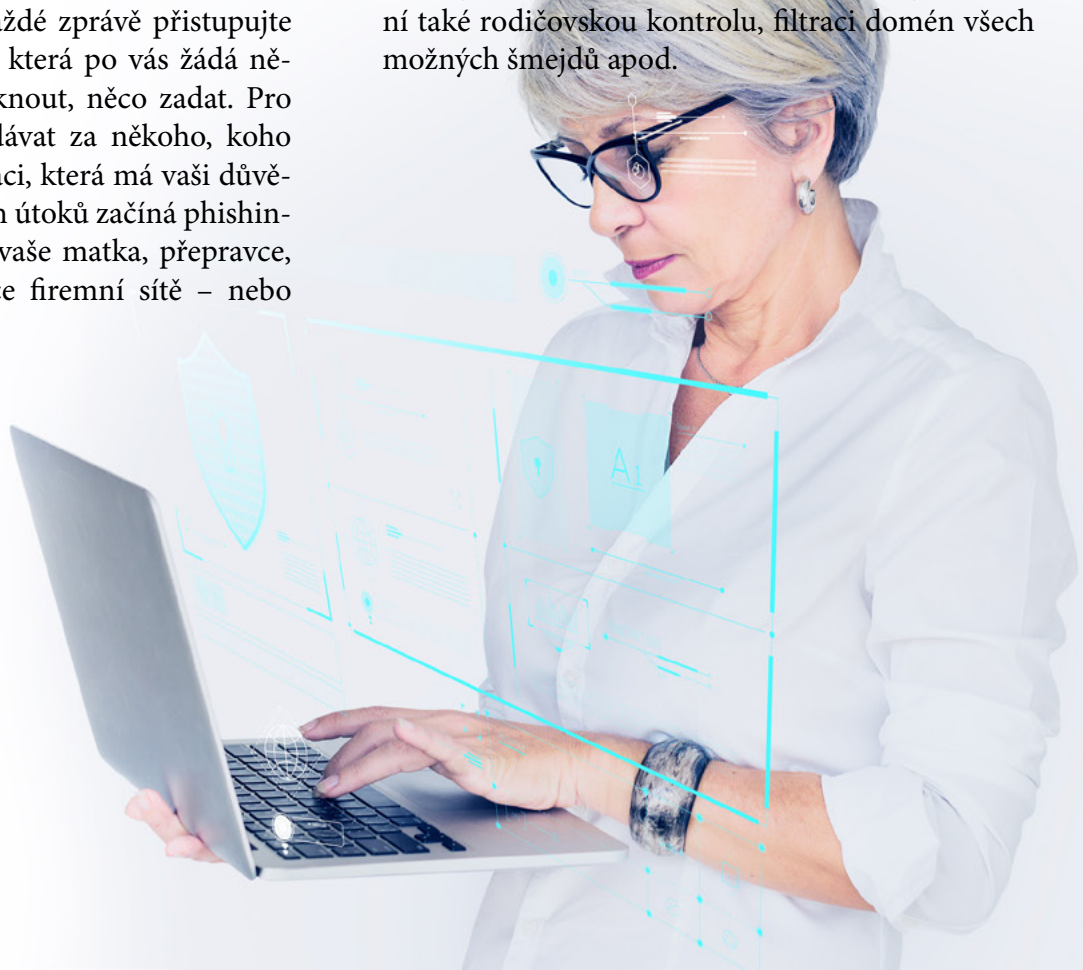
Nedůvěřujte nikomu. Ke každé zprávě přistupujte s nedůvěrou. Zejména k té, která po vás žádá nějakou aktivitu – někam kliknout, něco zadat. Pro hackery není složité se vydávat za někoho, koho znáte osobně, nebo organizaci, která má vaši důvěru. Více jak 90% hackerských útoků začíná phishingem. Ať už je odesílatelem vaše matka, přepravce, lékař, lékárník nebo správce firemní sítě – nebo kdokoli jiný, vždy buďte pozorní nejen vůči formě (obvyklý formát zprávy, hlavička, podpis, grafika), ale také obsahu (je možné, aby mi právě tohle psala moje matka?). Nikdy nepodléhejte časovému tlaku (je třeba okamžitě změnit vaše heslo do cloudové služby zde). V takových zprávách nikdy neklikejte na odkazy! Pokud budete mít jakékoliv podezření, neváhejte odesílateli zavolat a ověřit si, že zprávu skutečně posílal on.

9. Nechoď na internetové stránky, o kterých víš, že nejsou legální

Pokud někdo provozuje nelegální stránku, je jasné, že si nebude dělat těžkou hlavu ani s vaší bezpečností. Obvykle jde o služby, které jsou mimo zákon. Existuje reálná možnost nákazy už při jejich otevření v prohlížeči. Odkazy pak mohou vést na další škodlivé stránky. Nebo stránky podvržené, které se vydávají za legální.

10. Dbej na bezpečnost zranitelných osob ve svém prostředí.

Jde o děti, seniory nebo osoby s omezenými schopnostmi, jejichž aktivity mohou vést k nebezpečnému chování online. Je důležité mít schopnosti a možnosti kontrolovat také jejich chování a bezpečnost. A pokud možno je vybavit pokročilejšími nástroji, které jejich ochranu zautomatizují. Umožní také rodičovskou kontrolu, filtraci domén všech možných šmejdů apod.



CO MUSÍM MÍT (POKUD MOŽNO) ZDARMA?

PRO ÚTOČNÍKA JE ZAJÍMAVÝ KAŽDÝ

Zapnutý antivirus

Jsem si jistý, že jde o samozřejmost, kterou není třeba zdůrazňovat. Minimálně tedy antivirus, kterým dodavatel operačního systému tento vybavil.

Zálohování

Je dobré udržovat minimálně jednu kopii vašich dat (raději ale více) na zařízení, které není připojené online k vašemu PC. To proto, aby v případě hackerského útoku neměl útočník přístup k vašim zálohám. Tím by bezpečnostní kopie pozbyly svůj smysl.

Velice doporučuji toto nenechávat na ručním kopírování, ale použít nástroj z operačního systému, který používáte, nebo ještě lépe profesionální aplikaci. Je jich hodně, existují i jejích žebříčky oblíbenosti. Doporučit lze třeba *SyncBackFree* nebo *FreeFileSync*.

Čas od času je dobré zálohy testovat – zkontrolovat, jestli jsou funkční (jde z nich obnovit soubor) a zda zálohování skutečně probíhá.

Správce hesel

O hygieně hesel již byla řeč. Tvořit a pamatovat si odolné heslo pro každou webovou stránku, aplikaci či uživatelský účet může být náročné. Dělat si poznámky – a ty pak někde zapomenout v otevřené formě může být zase nebezpečné. Pomůže vám šikovný správce hesel, který umožní hesla bezpečně uložit, sdílet s vašimi ostatními zařízeními a třeba i poradit s bezpečnou délkou. Mohu zmínit třeba *StickyPassword* v placené i free verzi.

Bezpečnou VPN

Nepoužívat nezabezpečenou WiFi síť je jednou ze zásad, které byly uvedeny v minulé kapitole. Pokud se tomu nedá vyhnout, je důležité použít bezpečnou VPN, tedy Virtuální Privátní Síť, kterou můžete používat i při připojení k nezabezpečené síti. Tu vám může poskytnou třeba zaměstnavatel (pokud tedy k tomu má důvod) nebo spolehlivý poskytovatel, který to ale neudělá zadarmo – protože k tomu musí využívat technickou infrastrukturu a správu, která něco stojí. Existují i VPN, které jsou zdarma – ty ale nelze považovat za bezpečné.

Díky této síti se můžete nejen připojit k internetu v nezabezpečené WiFi síti a třeba platit své účty. Můžete také využít virtuální změny vaší lokace – tedy připojit se online třeba z jiného města ve světě, kde má poskytovatel VPN přípojný bod. To může pomoci překonat regionální omezení některých služeb nebo se vyhnout odposlechu komunikace v zemích, kde si s tím vlády nelámou hlavu. Pokud byste chtěli VPN za rozumnou cenu, mohu doporučit *F-Secure Freedome*, která vás vyjde měsíčně na cca 28,- Kč.

Oddělené prostředí

V domácích sítích nejde o běžnou věc. Některé lepší routery, kterými jste připojeni k internetu, umožňují postavení více oddělených sítí, mezi kterými je omezeno spojení. Je tak možné celkem bezpečně oddělit návštěvy, kterým dáte přístup na internet nebo zařízení či uživatele, jejichž bezpečnost nemáte ve svých rukou – co se týče zařízení můžeme mít na mysli „chytré krabičky" IOT, kde často nelze provádět aktualizace a třeba měnit přístupové údaje. Nebo mobilní telefony, které nemají důvod sdílet jednu síť s vaším PC (a které jsou poměrně často zdrojem bezpečnostních problémů – o tom si ale řekneme někdy jindy). Nebo děti, které neustále hledají po internetu software na potenciálně nebezpečných místech, jako jsou torrenty, a vůbec vlezou kamkoliv.

Může jít opět o významné posílení vaší bezpečnosti – obzvlášť v situaci, kdy pracujete doma. Ještě důležitější je to v případě, že se připojujete z domova do podnikové sítě nebo k podnikovým cloudovým službám.

Pokud váš router toto umožňuje, je to jen věc jeho nastavení. Když si s tím poradíte sami, nemusí vás to stát ani korunu…

PLACENÉ NEBO ZDARMA?

Nikdo nechceme utrácet peníze zbytečně. Jak moc ale chcete věřit někomu, kdo vám nabídne získání bezpečnější funkcionality vašeho auta zdarma? Všichni jsme ke své činnosti nějak motivovaní, a zdarma je jen to, co může přinést finanční efekt nepřímo.

Ruku na srdce – taky jsem vám nabídnul tuto příručku zdarma – a přitom věřím, že si ke mně najdete cestu pro něco, co mi umožní vydělat peníze. A to je dobrý důvod. Kdyby tomu tak nebylo, měli byste přemýšlet, jaký je můj úmysl. Hodně přeháním, ale třeba nějaký hacker by mohl „chlácholit" čtenáře a motivovat je k tomu, že je zbytečné vydávat peníze za ochranu – a pak „posbírat" oběti.

Důležitý je moment odpovědnosti: když někomu platíte, má takový dodavatel také jistou odpovědnost vůči vám. Pokud dostanete něco zadarmo, je odpovědnost prakticky nevymahatelná.

V bezpečnosti tato slova platí dvojnásob. V situaci, kdy se stáváme na informačních technologiích de facto závislí, to platí mnohonásobně.

Doporučuji tedy pečlivě zvážit, co budu používat zdarma a kde si raději připlatím.

Osobně bych volil jako placenou službu alespoň:

- ochranu proti pokročilým hrozbám – ideálně pohromadě s antivirovou ochranou,
- bezpečnou VPN.

Na stránce home.antihacker.cz/10rad najdete odkazy na výše uvedené způsoby placené ochrany, většinu z nich si můžete vyzkoušet po omezenou dobu zdarma. Na uvedené stránce najdete i další odkazy, které zmiňuji v této příručce.

ZAPOMEŇTE NA TO, ŽE PATŘÍTE MEZI TY, KTERÉ BY HACKERSKÝ ÚTOK NEPOŠKODIL!

Stále se setkávám s názory, kdy si člověk myslí, že jej hackerský útok nemůže poškodit. Nejčastější důvody pro takové tvrzení jsou:

- Na svých účtech mám minimum peněz, takže nejsem pro útočníka zajímavý.
- Jsem člověk, jehož osobní údaje nemohou nikoho zajímat.
- E-maily a další elektronická komunikace je tak jako tak otevřená, takže si nedělám hlavu s bezpečností.
- Hackerský útok, který by ochromil moje PC, by byl nepříjemný, ale nemyslím si, že by mne skutečně mohl poškodit.

Tak jednoduché to není: pro útočníka je zajímavý každý – i člověk zcela bez majetku. Pokud skutečně nenajde žádnou finanční hodnotu, může třeba ukrást vaši identitu, vydávat se za vás, vaším jménem rozesílat podvodné e-maily anebo třeba pod vaší identitou provádět trestnou činnost. To už rozhodně není legrace! Přece nikomu nedáte svůj občanský průkaz! Jeho hodnota je určitě malá, ale zločinec s tím dokáže provádět nepěkné věci.

Může toho dělat ještě více – o tom si řekneme jindy. Sledujte naše webové stránky a blog.

ZÁVĚR: KONTROLNÍ SEZNAM.

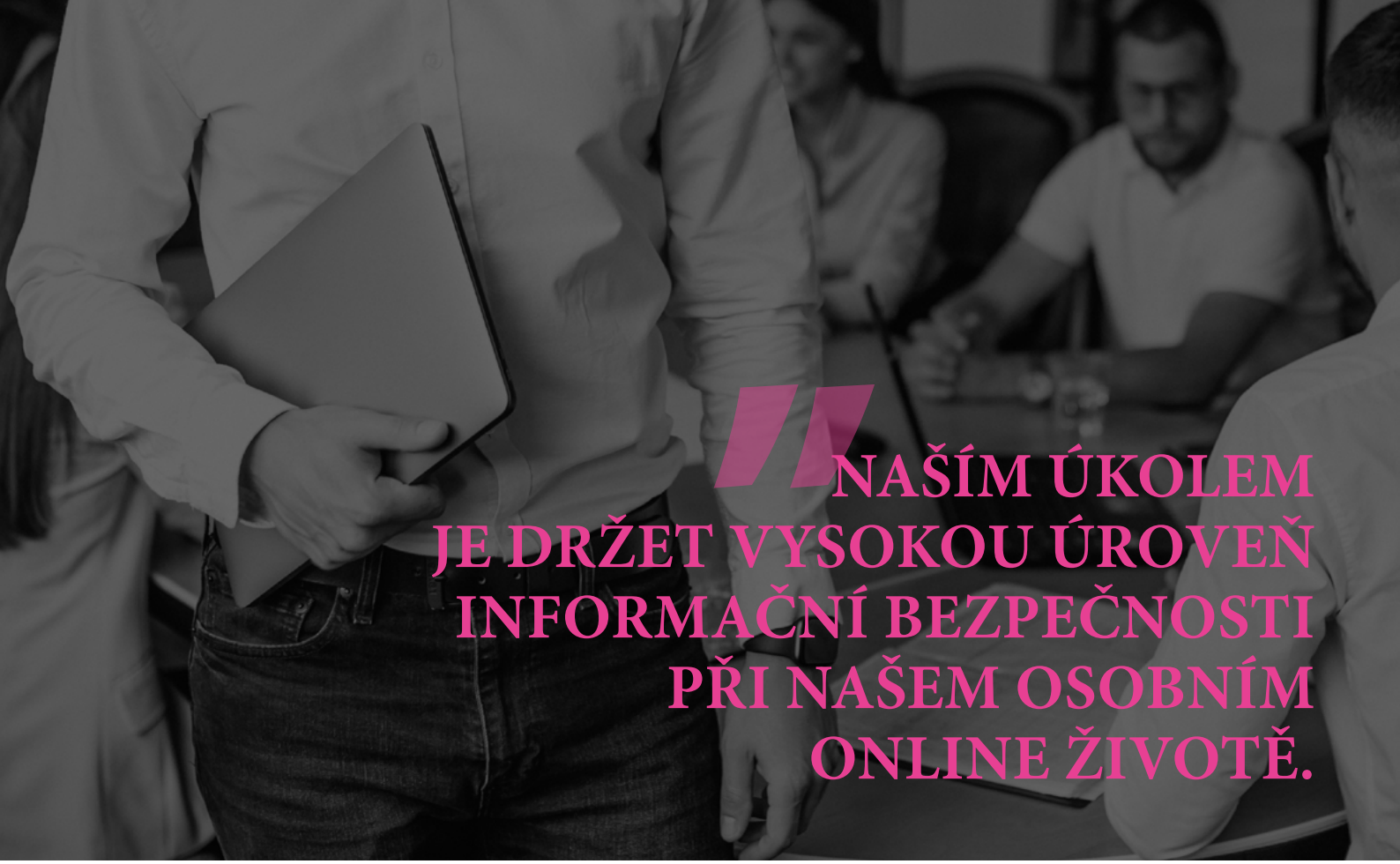
Podle Wikipedie jde o druh pracovní pomůcky používaný ke snížení selhání kompenzací potenciálních limitů lidské paměti a pozornosti. Pomáhá zajistit konzistenci a úplnost při provádění úkolu.
Ano, to je jistě správně. Naším úkolem je držet vysokou úroveň informační bezpečnosti při našem osobním online životě. Už jsme si řekli, že je to úkol obtížný, protože se nám neustále mění okolí a prostředí hrozeb. Proto je vhodné vytvořit kontrolní seznam, který by nám občas připomněl, co je třeba dělat, a pomohl zkontrolovat, zda jsme něco neopomněli. Nabídnu vám tento:

VÍM, O CO JDE, A JSEM PŘESVĚDČEN, ŽE:	✔
Nepoužívám nechráněné WiFi sítě.	
Chráním svoje osobní údaje.	
Používám jedinečná a odolná hesla.	
Vyhýbám se recyklaci svých přístupových údajů.	
Mám představu o tom, jak se chovají ostatní uživatelé mojí domácí sítě a že také dodržují tyto zásady.	
Svoje systémy mám stále aktuální, aktualizace provádím co nejdříve po jejich vydání.	
Na svém PC nepracuji pod administrátorským oprávněním.	
Jsem pozorný ke zprávám, co chodí do mojí e-mailové schránky, neklikám na podezřelé odkazy.	
Nechodím na nelegální webové stránky.	
Dbám na bezpečnost zranitelných osob v naší síti.	
Mám zapnutý antivirus.	
Zálohuji svoje data na dvě zařízení, která nejsou trvale připojená k mému PC.	

3 body, které na které je dobré odpovědět ANO:

Používám bezpečného správce hesel.	
Používám bezpečnou VPN.	
Mám oddělené prostředí domácí sítě.	

čas podíváte – prostředí online hrozeb se vyvíjí rychle a naše požadavky na online služby jdou také dopředu. Tím se mění také potřeba se chránit, která nebyla nikdy v minulosti tak naléhavá, jako dnes.



„NAŠÍM ÚKOLEM JE DRŽET VYSOKOU ÚROVEŇ INFORMAČNÍ BEZPEČNOSTI PŘI NAŠEM OSOBNÍM ONLINE ŽIVOTĚ.

NEJLEPŠÍ NAKONEC

Jsem skutečně rád, že jste dočetli až sem.
A budu ještě radši, když vám moje rady poslouží k většímu bezpečí a pohodě. Tedy nejen k pocitu, ale skutečně!

Budete-li chtít, mohu vám nabídnout:

- E-book „Informační bezpečnost pro domácí uživatele a malé kanceláře“
- Články na blogu
- Vyzkoušení produktů pro ochranu online zdarma
- Prodej těchto produktů a podporu při použití
- Odběr newsletteru

Bezpečí a pohodu (nejen) v online životě přeje

Josef Javora

Všímavému čtenáři jistě neušlo, že jsem sliboval 10+1 radu a v textu jich bylo zatím jen deset. Zde je ta poslední:

11. Buď krok před ostatními.

Tak jako je tomu v ochraně majetku – třeba obydlí: zloději nekradou nejčastěji v domech a vilách, které se zdají být nejbohatší (a tedy nejlépe zabezpečeny) – ale především tam, kde je to pro ně nejsnadnější, tedy v těch nejhůře zabezpečených. V online prostředí je to stejné. Je tedy lepší, abychom byli zabezpečeni nadprůměrně. Pak se pravděpodobnost útoku na nás rasantně snižuje. Právě o to nám jde. A to je hlavní důvod, proč jsem přinesl na náš trh ochranu proti pokročilým hrozbám Heimdal Security. Je pro útočníky velkou komplikací na jejich cestě k penězům. Ale těch méně zabezpečených je stále dost a dost…

Získali jste tento e-book od někoho jiného, než přímo od nás? Jsem rád, jestli se Vám líbil - pokud se zaregistrujete na adrese safe.antihacker.cz.
Dostanete nejen svou vlastní kopii e-booku, ale také v 10 e-mailech sadu videí, které Vás v informační bezpečnosti posunou zase o kus dále a k tomu získáte možnost vyzkoušet pokročilé prvky ochrany zdarma. Nic Vás to nebude stát!

TISPARTNERS
TRUSTED INFORMATION SECURITY