69 Kč / KVĚTEN 2020 / číslo 21

Kyberstalking od roku 2010 jako trestný čin.

Buďte na internetu v bezpečí. Víte, jak se chovat?

MAGAZÍN

MILENIÁL

TÉMA:

BEZPEČNOST NA INTERNETU

EXISTUJE NÁVOD NA ZABEZPEČENÍ?
A JAK SE MŮŽEME CHRÁNIT MY SAMI?

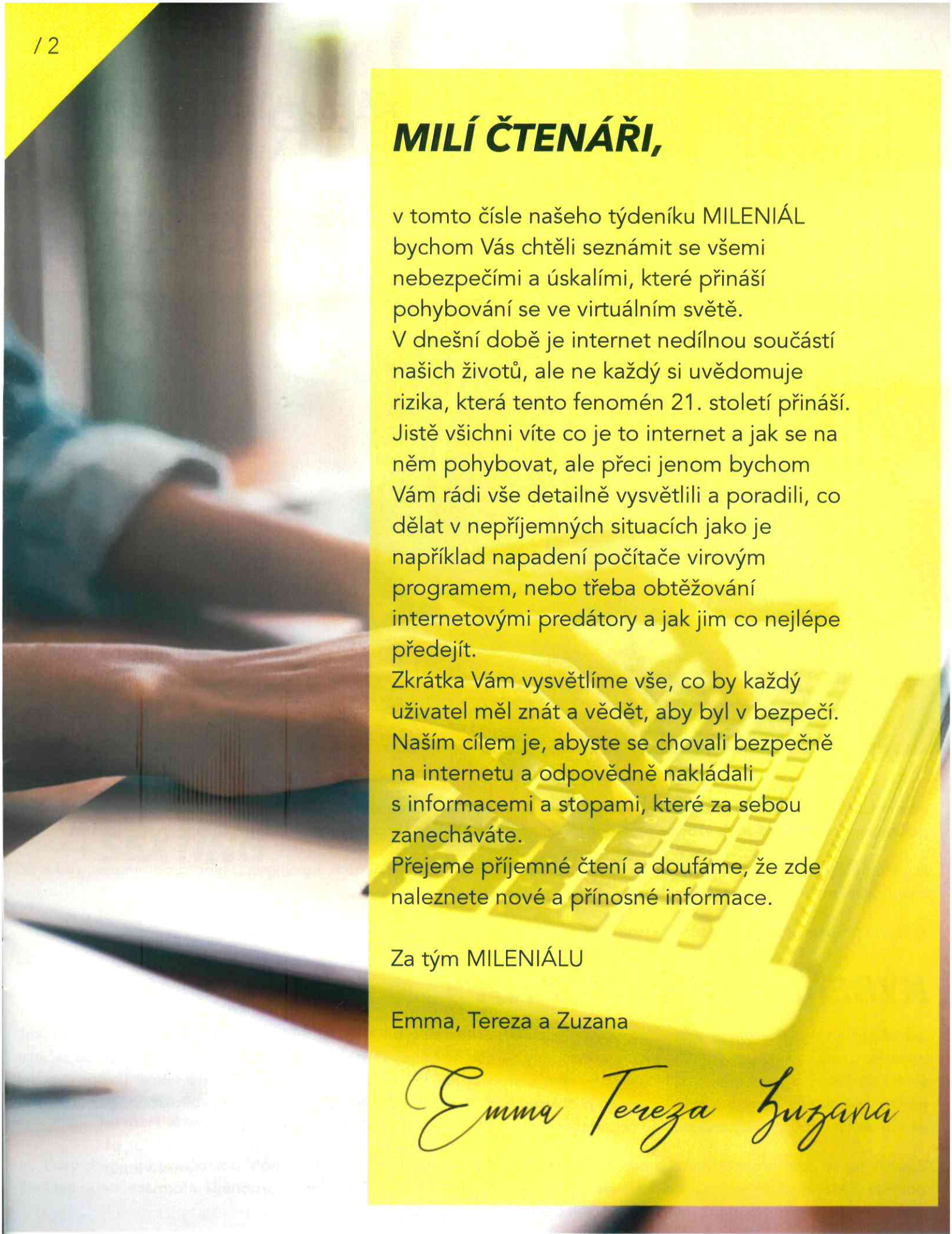
V SÍTI

RECENZE DOKUMENTÁRNÍHO FILMU BARBORY CHALUPOVÉ A VÍTA KLUSÁKA.

VELKÉ SROVNÁNÍ ANTIVIROVÝCH PROGRAMŮ

KTERÝ JE PRÁVĚ TEN NEJLEPŠÍ? A JAKÉ FUNKCE MÁ VLASTNĚ ANTIVIROVÝ PROGRAM?

OBSAH



MILÍ ČTENÁŘI,

v tomto čísle našeho týdeníku MILENIÁL bychom Vás chtěli seznámit se všemi nebezpečími a úskalími, které přináší pohybování se ve virtuálním světě.
V dnešní době je internet nedílnou součástí našich životů, ale ne každý si uvědomuje rizika, která tento fenomén 21. století přináší.
Jistě všichni víte co je to internet a jak se na něm pohybovat, ale přeci jenom bychom Vám rádi vše detailně vysvětlili a poradili, co dělat v nepříjemných situacích jako je například napadení počítače virovým programem, nebo třeba obtěžování internetovými predátory a jak jim co nejlépe předejít.
Zkrátka Vám vysvětlíme vše, co by každý uživatel měl znát a vědět, aby byl v bezpečí.
Naším cílem je, abyste se chovali bezpečně na internetu a odpovědně nakládali s informacemi a stopami, které za sebou zanecháváte.
Přejeme příjemné čtení a doufáme, že zde naleznete nové a přínosné informace.

Za tým MILENIÁLU

Emma, Tereza a Zuzana

Emma Tereza Zuzana

RIZIKA NA INTERNETU

A INTERNETOVÍ HACKERS

Internet nás může přivést do spousty různých situací, které nás můžou ohrozit. At už je to ohrožení softwaru domácího počítače nebo našich životů, vždy se proti nim můžeme nějak chránit, nebo jim zodpovědným chováním předcházet.

Konkrétně bychom se mohli setkat s kybernetickou šikanou, kyberstalkingem, sextingem, kybergroomingem, rizika při nakupování on-line, phishingem nebo viry.

Krátce si představíme, co tato témata jsou, a co pro napadené znamenají a jak vůbec vznikla.

KYBERNETICKÁ ŠIKANA

Jak už plyne z názvu jedná se o šikanu v digitálním prostředí, neboli cyberbullying. Šikanu známe primárně z prostředí škol, proto jsou nejčastěji touto digitální šikanou napadeny děti, jelikož dnes většina z nich má přístup k internetu již od začátku školní docházky a je mnohem jednodušší někoho šikanovat na dálku, než osobně. Děti, jakožto lehce manipulovatelní jedinci, se neumějí bránit a často se o tomto problému bojí mluvit. Ale děti nejsou jediné oběti kybernetické šikany. Můžou se s ní setkat i dospělé osoby. Cílem je napadeného zesměšnit, ztrapnit, zastrašit a celkově oběti ublížit.

Zásadní je, se proti ní umět bránit a nejlépe šikanátora nahlásit policii, aby v tom nemohl pokračovat i u jiných osob. Je potřeba posbírat co nejvíce důkazů o šikaně a zajistit bezpečí svědku, kteří poskytli podrobnější informace, nebo nahlásili podezření o šikaně a následně tento případ řešit s policií.

KYBERSTALKING

Jde o sledování a obtěžování někoho online. Stalker získává informace o své oběti hlavně z jeho příspěvků na sociálních sítích. Dnes je velice snadné získat osobní informace o našem životě, jelikož velké procento populace se zveřejňuje na svých profilech, kam například chodí na obědy, kde bydlí, v kolik chodí spát atd. Může to být například ublížený pronásledovatel, milovník, který si myslí, že ho oběť miluje, bývalý partner nebo sexuální deviant. Nejčastějšími obětmi jsou celebrity, známé osobnosti jako třeba politici, nebo také expartneři. Od roku 2010 je kyberstalking trestným činem.

JAK SE PROTI KYBERSTALKINGU BRÁNIT?

- Neodpovídejte stalkerovi na zprávy a rozhodně nechoďte na žádné schůzky

- Změňte své denní rutiny. Např. kam chodíte do restaurace, na nákupy atd.

- Schovejte si důkazy v podobě výhružných SMS nebo emailů

- Zablokujte stalkera na všech svých sociálních sítích

- Nebojte se o tomto problému mluvit se svými blízkými a informovat je o tom

SEXTING

Při sextingu jde o dobrovolné sdílení intimních fotografií, videí a intimních textových zpráv. V případě, že se partneři, u kterých proběhl sexting rozejdou, může z jedné strany dojít ke zveřejnění intimního materiálu za účelem pomsty, vydírání, nebo šikany. I když lechtivé fotografie nepošlete, ve vašem telefonu a počítači nejsou úplně v bezpečí, někdo může váš počítač hacknout a dostat se s těmto materiálům. Když už někdo sexting provozuje, měl by si dávat pozor, aby nebylo možné ho identifikovat a už vůbec by mu nemělo být vidět do obličeje. Nejbezpečnější sexting vůbec neprovozovat.

KYBERGROOMING

V tomto případě bývají obětmi nejčastěji děti a dospívající. Útočník se pod falešou identitou snaží sblížit vybranou osobou online, s cílem osobního setkání, při kterém následně může dojít k sexuálnímu zneužití.

PŘÍPAD KYBERGROOMINGU

Usvědčený deviant, vrátný v tiskárnách, Pavel H. používal k seznamování se s oběťmi diskuzní fóra, chaty i inzeráty. Nejčastěji předstíral, že děti z dětských domovů vybírá do soutěže Dítě VIP. Osobní informace a fotografie, které od dětí získal, pak použil k vydírání. Kombinací vydírání a uplácení přiměl některé děti k osobní schůzce.

- Důsledek: Znásilnil a zneužil dvacet chlapců. Byl uvězněn na 8 let.

Kam se můžete obrátit pro pomoc?

Pomoc online – linka bezpečí online
- pomoc@linkabezpeci.cz
- telefon: 116 111

Online poradna E-Bezpečí
- www.napisnam.cz

RIZIKA PŘI NAKUPOVÁNÍ ONLINE

Při nakupování online můžete narazit na podvodné eshopy, které vás okradou a nedodají zboží. Tomu lze ale celkem snadno předejít:

Ověřte si doménu, kontaktní informace a smluvní podmínky. Pokud prodávají zboží za neuvěřitelně nízké ceny, téměř vždy se jedná o podvod. Najděte si recenze na daný eshop a nikdy neplatte převodem na účet. U nákupu ze zahraničí si dávejte pozor na nutnost zaplatit clo a DPH, protože může jít o hodně vysoké částky.

PHISHING

U tohoto typu napadení vašeho soukromí se útočník snaží svou oběť nalákat pomocí falešného e-mailu, nebo internetové reklamy.

Oběť si myslí, že jí přišel třeba e-mail od banky. V domnění, že je to opravdu jeho banka e-mail otevře a ten ho přesměruje na web, kam musí vyplnit své přihlašovací údaje a zloděj vzápětí vykrade bankovní účet.

Dnešní prohlížeče umí varovat, pokud se chystáte vstoupit na phishingový web, ale ne vždy se na to můžete spolehout.

VIRUS

Původní myšlenka počítačového viru byla, dostat se do počítače a dál se šířit. V dřívějších dobách prostě smazal vše, co se v počítači vyskytovalo.

TROJSKÝ KŮŇ ("TROJAN")

Škodlivý počítačový program, který má za cíl umožnit někomu cizímu dostat se někomu cizímu do počítače a získávat z něj údaje.

KEYLOGGER

Vir, který sleduje a zaznamenává, co píšete na klávesnici. To odesílá útočníkům.

RANSOMWARE

Počítačový systém napadený tímto typem viru se zablokuje nebo zašifruje, takže se jeho vlastník nedostane k ničemu, co v počítači má. Útočník se následně snaží svou "oběť" vydírat výhružnými zprávami a dožaduje se zaplacení výkupného.
Po zaplacení rozhodně nečekejte, že by vám útočník vše vrátil.

Výše uvedené hrozby na internetu jsou pouze kapkou v moři. Kterýmkoli z nebezpečných programů se může nakazit každé zařízení, které má přístup k internetu, tedy i váš mobilní telefon nebo tablet. Ochrana proti virům nespočívá jen v důsledném používání antivirových programů, ale také v obezřetném chování na síti.

Mějte v počítači i telefonu nainstalovaný spolehlivý antivirový program.

Nestahujte a neotevírejte přílohy z nedůvěryhodných a cizích e-mailů. **| Tereza**

HACKEŘI V GRAFECH

Internetoví hackeři nebo útočníci nesměřují své útoky pouze na velké firmy, ale obětí se může stát i obyčejný člověk, a to skrze e-mail, mobil nebo jiný přístroj, který je připojený k internetu.

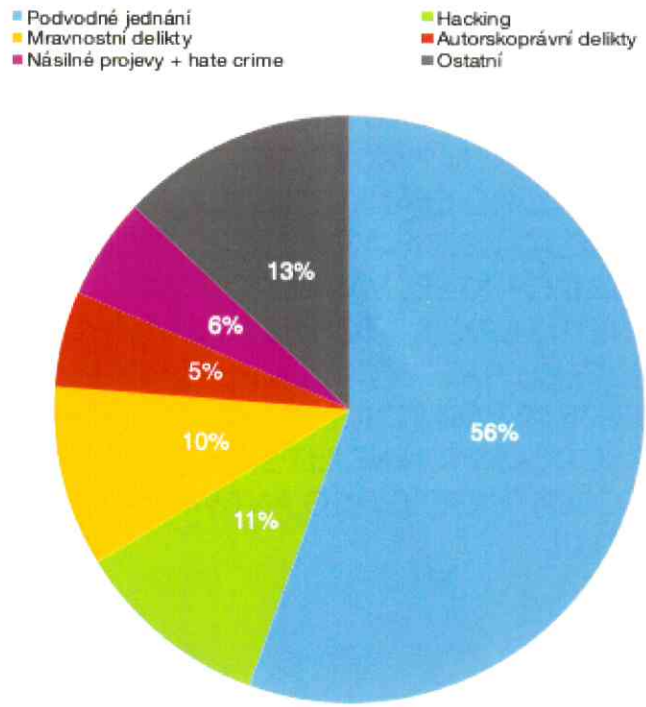
S krádeží informací nebo napadením počítače má zkušenost většina občanu u nás, ale také ve světě. V souvislosti s kybernetickou bezpečností se můžeme setkat se zkratkami CERT (Computer Emergency Response Team) a CSIRT (Computer Security Incident Response Team). Tyto organizace se zabývají řešením problému s oblasti kyberprostoru a na který se mohou uživatelé nebo jiné týmy obrátit s incidenty nebo podezřeními.

Nejznámější jsou trojské koně, které mají za úkol ukrást co nejvíce informací o účtech, kreditních kartách apod. Tyto kyberútoky je mnohem snazší zpeněžit - útočníci požadují po obětech výkupné a pomocí kryptoměn typu bitcoin či ethereum. Ransomware necílí pouze na firmy, ale na kohokoli, kdo uchovává nějaká data.

Oběťmi v minulosti byly nemocnice, orgány činné v trestním řízení, vládní agentury a orgány. Častými cíli jsou i malé a střední podniky, které často nemají dostatek prostředků k ochraně svých dat. Mezi lety 2015 a 2016 vzrostl počet ransomwarů o 750 %. **| Emma**

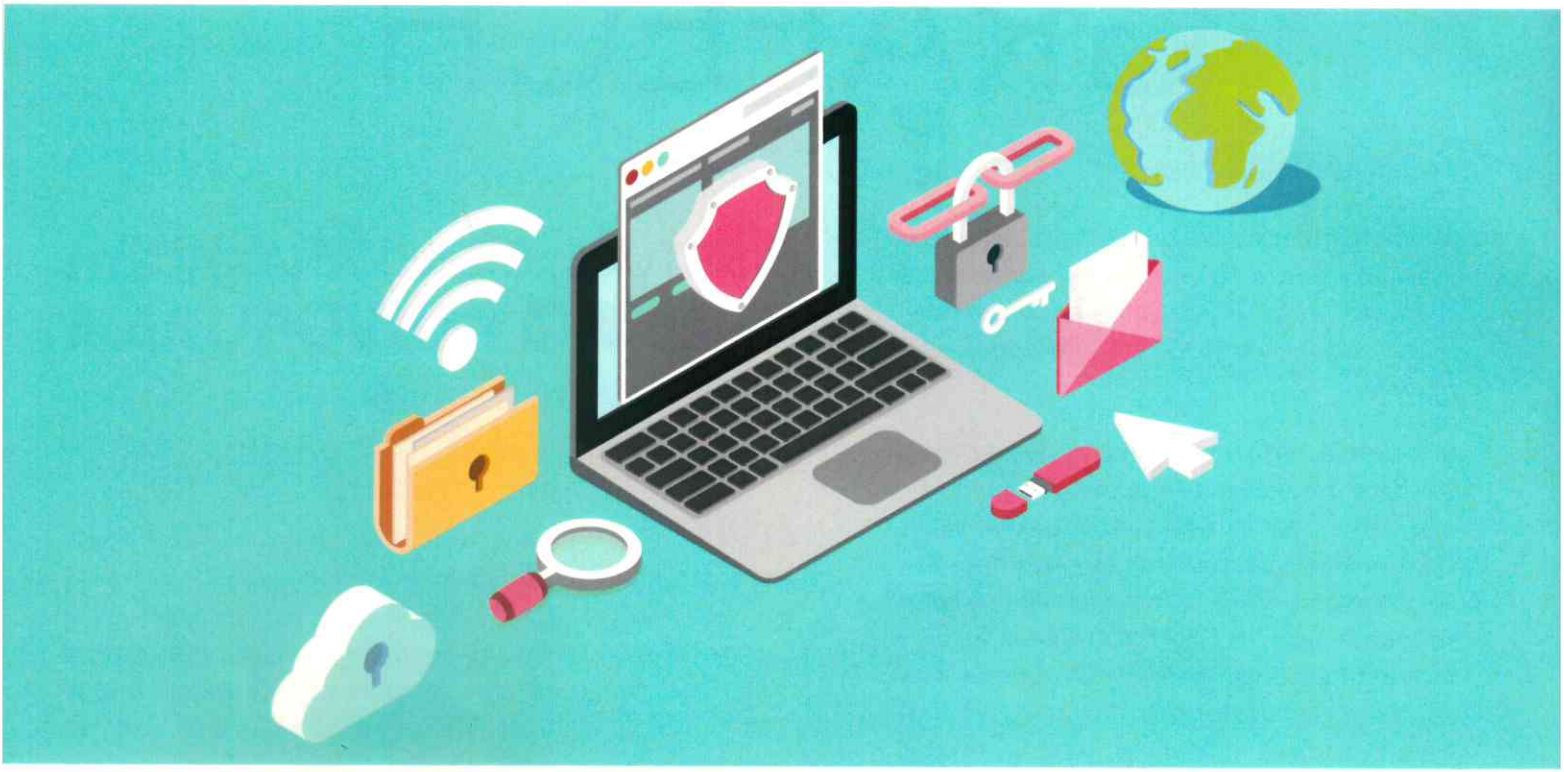
INSTITUCE, KTERÉ BÝVAJÍ NEJČASTĚJI NAPADENY:

1. Energetika (elektřina, plyn, ropa)
2. Doprava (letadla, železnice, vodní a silniční doprava)
3. Bankovnictví
4. Infrastruktura finančních trhů
5. Zdravotnictví
6. Zásoby a distribuce pitné vody
7. Digitální infrastruktura (e-shopy, internetová úložiště)



BEZPEČÍ NA INTERNETU

ZVANÉ ANTIVIROVÉ PROGRAMY



INTERNET JE SKVĚLÁ VĚC. USNADNIL NAŠE ŽIVOTY TAK, ŽE MNOHDY STAČÍ JEN JEDNI KLIKNUTÍ, ABYSTE POHODLNĚ ZAŘÍDILI VŠECHNO, CO POTŘEBUJETE, AŤ UŽ SE JEDNÁ O PRÁCI, ŠKOLU NEBO ZÁBAVU. ALE OPATRNOSTI NENÍ NIKDY DOST.
Z PŘEDCHOZÍHO ČLÁNKU JSTE SE DOZVĚDĚLI O NEJZÁVAŽNĚJŠÍCH PROBLÉMECH, KTERÉ VÁS MŮŽOU NA INTERNETU POTKAT. Z TOHO DŮVODU BYLY VYVINUTY CHYTRÉ ANTIVIROVÉ PROGRAMY. POKUSÍME SE VÁM POSKYTNOUT SHRNUTÍ A POPIS SOUČASNÝCH NEJLEPŠÍCH SPOLEČNOSTÍ, KTERÉ TYTO ANTIVIRY POSKYTUJÍ.

Při nákupu odpovídajícího programu sehrává roli hned několik kritérií. Zjistěte si úroveň skeneru, rezidentního štítu a rychlost aktualizací, uživatelskou přívětivost programu, jeho hardwarové nároky a dostupnost podpory. Vzhledem k tomu, že mnohé společnosti nabízejí i placené verze, promyslete si dobře, zda jejich služeb využijete.

SKENER A REZIDENTNÍ ŠTÍT

Skenerem a rezidentním štítem jsou vybaveny nejlepší antivirové programy. Skener aktivně pátrá po hrozbách, které se již na disku nacházejí, a stará se o jejich likvidaci. Jeho efektivita musí činit alespoň 90 %, abyste měli dostatečnou jistotu.

Rezidentní štít představuje online ochranu. Neustále monitoruje veškerou činnost uživatele na internetu i v počítači. Jeho účinnost musí dosahovat alespoň 80 %.

RYCHLOST AKTUALIZACÍ

Pokud se vyskytne nový druh viru, tato funkce by měla v co nejkratším čase získat potřebnou aktualizaci.

HARDWAROVÉ NÁROKY

Pokud se jedná o aplikaci, která vyžaduje výraznou pomoc výpočetního výkonu. V optimálním případě **by neměla být činnost antiviru vůbec znát.**

V případě, že program má vysoké nároky na hardwarovou pomoc, může se stát, že počítač se rapidně zpomalí, protože je zaměstnán antivirovou kontrolou a tak otevření obyčejného okna prohlížeče je najednou záležitostí na několik minut.

PODPORA

V případě nějakého problému s Vaším antivirovým programem se vyplatí vědět, že se můžete někam obrátit s dotazem nebo žádostí o řešení problémů. Většina firem podporuje kromě klasické **emailové adresy** také **přímou mobilní infolinku** nebo **live chat**.

NÁZEV ANTIVIROVÉHO PROGRAMU	Avast	AVG Internet Security	Norton Security	Kaspersky	ESET Smart Security
ZABEZPEČENÍ WEBKAMERY	×	✔	✔	nízké	✔
HARDWAROVÉ NÁROKY	nízké	nízké	střední		nízké
TELEFONICKÁ PODPORA V ČEŠTINĚ	✔	×	×	×	✔
OBSLUHA	snadná	snadná	náročná	snadná	snadná
OCHRANA PLATEB	✔	✔	✔	✔	✔
FIREWALL	✔	✔	✔	✔	✔
SPRÁVCE HESEL	✔	×	✔	×	×
ANTISPAM	✔	✔	×	✔	✔
ÚČINNOST SKENERU A REZIDENTNÍHO ŠTÍTU	vysoká	vysoká	vysoká	vysoká	vysoká
CENA ZA 1 ROK	1 190 Kč	1 199 Kč	790 Kč	800 Kč	1 490 Kč

VERZE PLACENÁ NEBO ZDARMA?

Všechny uvedené společnosti poskytují bezplatné verze antivirových programů, ale placené verze přeci jen pomáhají zamezit obrovským škodám, tím pádem jsou ve svém důsledku úspornější. Kromě standardních funkcí, kterými jsou vybaveny i bezplatné systémy, navíc nabízejí také správce hesel, pokročilejší skenery, ochranu proti spamu a krádežím citlivých údajů.

Máte-li na pevném disku uložena důležitá data a pracujete-li s citlivými údaji, doporučujeme raději investovat a zakoupit si placenou verzi programy.

JAK NAINSTALOVAT ANTIVIROVÝ PROGRAM V SYSTÉMU WINDOWS

Bez ohledu na to, **který antivirový program jste si vybrali,** nastavení a instalace v systému Windows je obvykle velice podobná.

1. Někteří poskytovatelé po vás nebudou požadovat, abyste se zaregistrovali hned, ale nutnost registrace bude do 30 dnů od zakoupení. Vytvoření účtu vám umožní přímý přístup k aktualizacím a místo, kde můžete spravovat další funkce.

2. Klepnutím stáhnete antivirový program. Potřebujete na něj ve svém počítači dostatečné množství místa, a proto vás o tom obvykle software informuj

3. Instalace softwaru bude vyžadovat autorizaci. Je to zadání hesla prostřednictvím účtu administrátora.

4. Postupujte podle návodu instalace na obrazovce

Software vás provede krátkým procesem instalace, který obvykle obsahuje přijetí podmínek a určení, kde bude antivirový program uložen.

5. Verze, kterou stáhnete, nemusí být nejaktuálnější verzí softwaru. S tím se vypořádáte jednoduše tak, že restartujte počítač. Jakmile je tento proces dokončen, spusťte v počítači kompletní skenování.

JAK INSTALOVAT ANTIVIROVÝ PROGRAM NA MAC

Jakmile najdete antivirový nebo bezpečnostní balík, který je kompatibilní s Macem, následujte stejný postup nastavení počítače jako u počítače se systémem Windows.

TIP PRO ANTIVIROVÉ PROGRAMY PRO MAC:

Avira – číslo 1 pro rok 2020. Doplňkové funkcí, jako je VPN a zabezpečený webový prohlížeč na ochranu před phishingovými útoky.

Sophos – Obsahuje funkce webové ochrany a je snadné jej nastavit a používat.

Bitdefender – jednoduchý software.

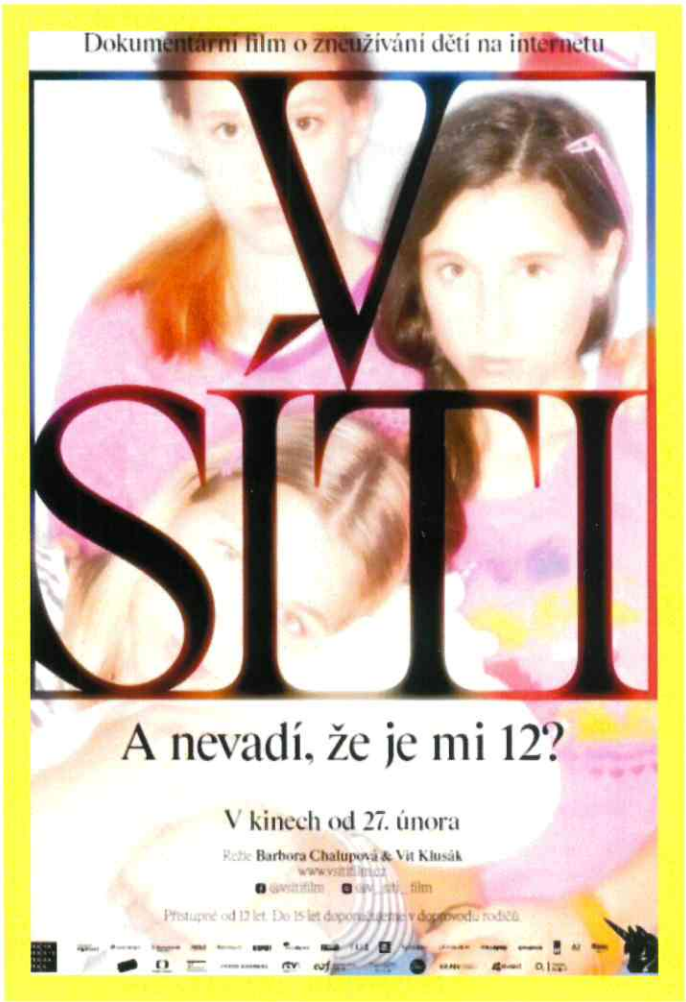
| Tereza

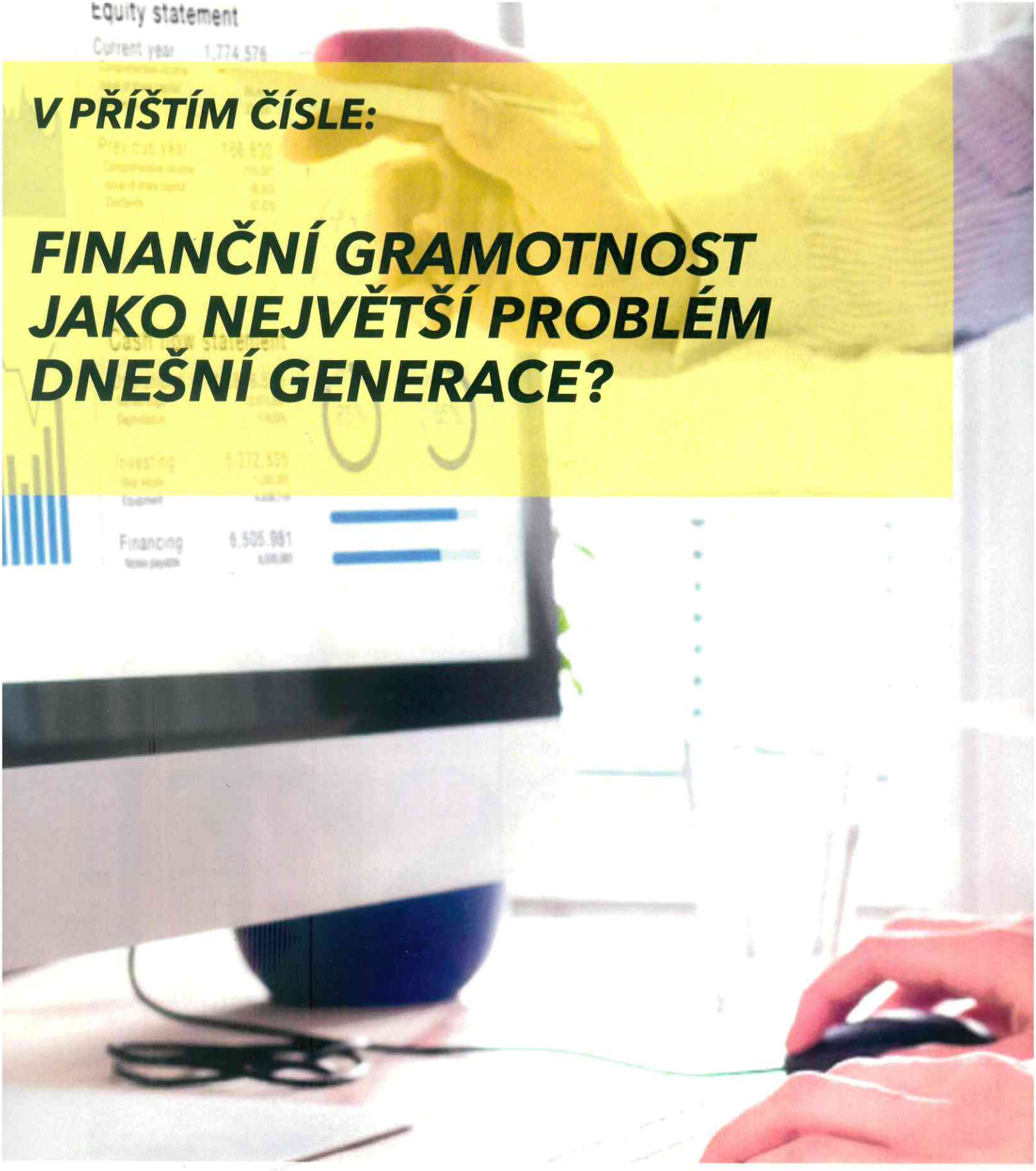
V SÍTI

3 herečky, 3 pokojíčky, 10 dní a 2458 potenciálních sexuálních predátorů. Radikální experiment otevírá tabuizované téma zneužívání dětí na internetu. Tři dospělé herečky s dětskými rysy se vydávají na sociální sítě, aby v přímém přenosu prožily zkušenost dvanáctiletých dívek online. Ve věrných kopiích dětských pokojů chatují a skypují s muži, kteří je na netu aktivně vyhledali a oslovili. Drtivá většina těchto mužů požaduje sex přes webkameru, posílá fotky svých penisů a odkazy na porno. Děti jsou dokonce vystaveny vydírání. Dokumentární film Barbory Chalupové a Víta Klusáka vypráví strhující drama tří hrdinek alias „dvanáctiletých dívek", pro které se účast na experimentu, od castingu až po osobní schůzky s predátory pod dozorem ochranky, stává zásadní životní zkušeností. Predátorské taktiky se postupně obracejí proti svým strůjcům: Z lovců se stávají lovení. (www.csfd.cz)

NAŠE RECENZE

Film V sítí perfektně zobrazuje, jak snadno se malé děti na internetu mohou stát terčem pedofilů a různých násilník. V dnešní době je totiž velice snadné se dostat a připojit se k různým serverům nebo do chatovacích místností a začít si psát prakticky s kýmkoliv. Nejrizikovější skupinou jsou v tomto ohledu děti, které jsou důvěřivé a netuší, co to může mít za následky. Ve filmu je přímo zobrazena trojice dívek, které se připojí na internetovou seznamku lide.cz a hned jim začnou psát náhodní muži různých věkových kategorií a požadovat po nich fotky s nevhodným obsahem. Když s nimi dívky zahájí videochat, někteří muži před nimi onanují. Jednoho z mužů pozná člen natáčecího štábu a dozvídáme se, že je vedoucím na táborech. Dalšímu agresorovi za přímluvu poslala jedna z dívek nahé fotky, které byli za pomocí fotomontáže vytvořeny k těmto účelům, a o onen muž ji začal vydírat, že jestli mu nepošle další, tak je zveřejní. Ve filmu pak také dojde na osobní setkání, kdy jeden manželský pár láká dívku k sexuálním praktikám. Podle mého názoru by tento film měli vidět jak rodiče tak i děti a pokusit se co nejvíc předcházet rizikům, které dětem na internetu hrozí. **| Emma**





V PŘÍŠTÍM ČÍSLE:

FINANČNÍ GRAMOTNOST JAKO NEJVĚTŠÍ PROBLÉM DNEŠNÍ GENERACE?

DRTINOVA

STŘEDNÍ ODBORNÁ ŠKOLA

Redaktorky:
Tereza Škodová
Emma-Cornelia Kempny

Grafika:
Zuzana Vladařová

4.B