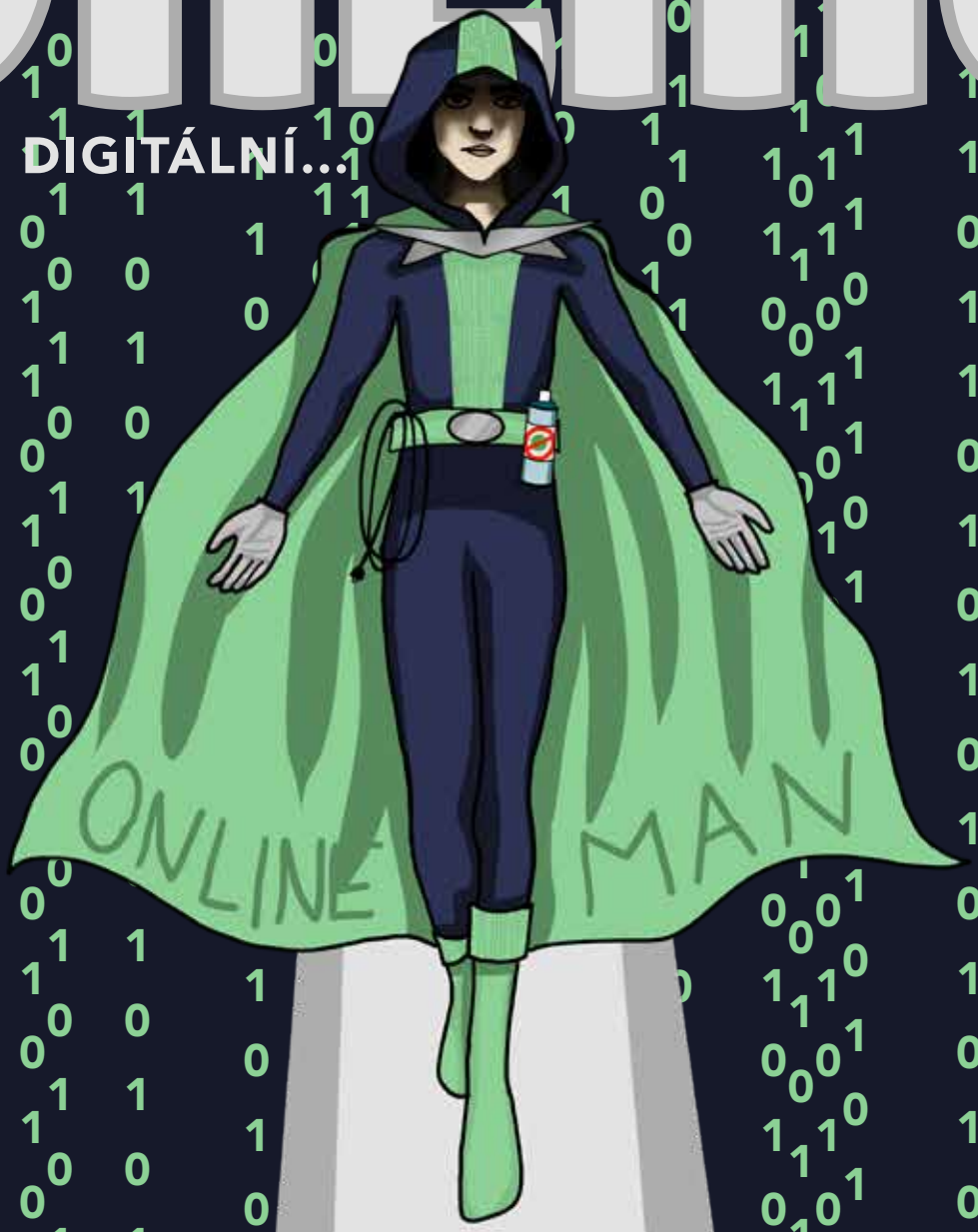
OnLine

V DOBĚ DIGITÁLNÍ...



KVĚTEN 2020

HACKERSKÉ TECHNIKY • PHISHING • KYBERŠIKANA • ANTIVIRUS • HTTP A HTTPS
ONLINE NAKUPOVÁNÍ • ONLINE BEZPEČÍ • FIREWALL • ZABEZPEČENÍ POČÍTAČE

Vážení čtenáři,

představujeme Vám časopis OnLine, který se zabývá kyberprostorem. Vysvětlíme Vám, jak funguje phishing, firewall nebo proč si zvolit stránky uvedené slovem HTTPS. Najdete v něm články s radami, jak chránit svůj počítač před nebezpečím, kterému čelí pravidelným užíváním nebo také doporučení o ochraně pro uživatele.

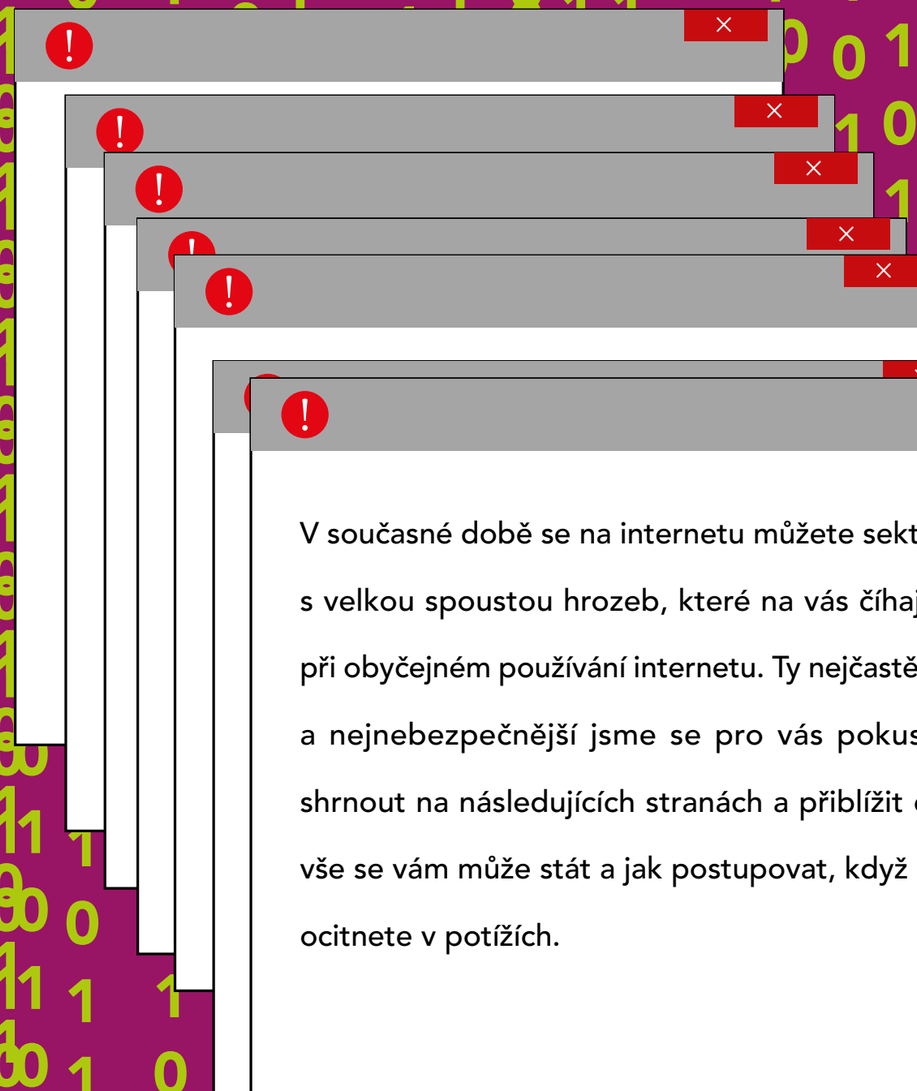
Zaměřili jsme se především na základní pojmy a doporučení, která by se hodila znát každému uživateli chytrých zařízení. Po celou dobu čtení Vás budeme doprovázet. Tak se na to pojďme společně podívat!

OBSAH

REDAKCE

Redakční tým našeho časopisu **OnLine** tvoří tři studentky Obchodní Akademie v Českých Budějovicích. Jednotlivé články si pro vás připravily **Barbora Popielová**, která vám představí nástrahy Kyberšikany, poučí vás v online bezpečnosti a ukáže vám, co je to Firewall. **Tereza Stehlíková** vás seznámí s návodem jak si zabezpečit zařízení a jaké používat antiviry, nebo co je vlasně http a https. Poslední z redakčního týmu si připravila několik článků **Tereza Trnková**. Ta se vám pokusí přiblížit co je to Phishing, a jak pracují hackeři. Společně s Bárou se ještě ponořily do problematiky nakupování na internetu. Tereza také stojí za grafickou stránkou časopisu včetně ilustrací a nakonec si pro bystré čtenáře připravila tajenku.

HROZBY

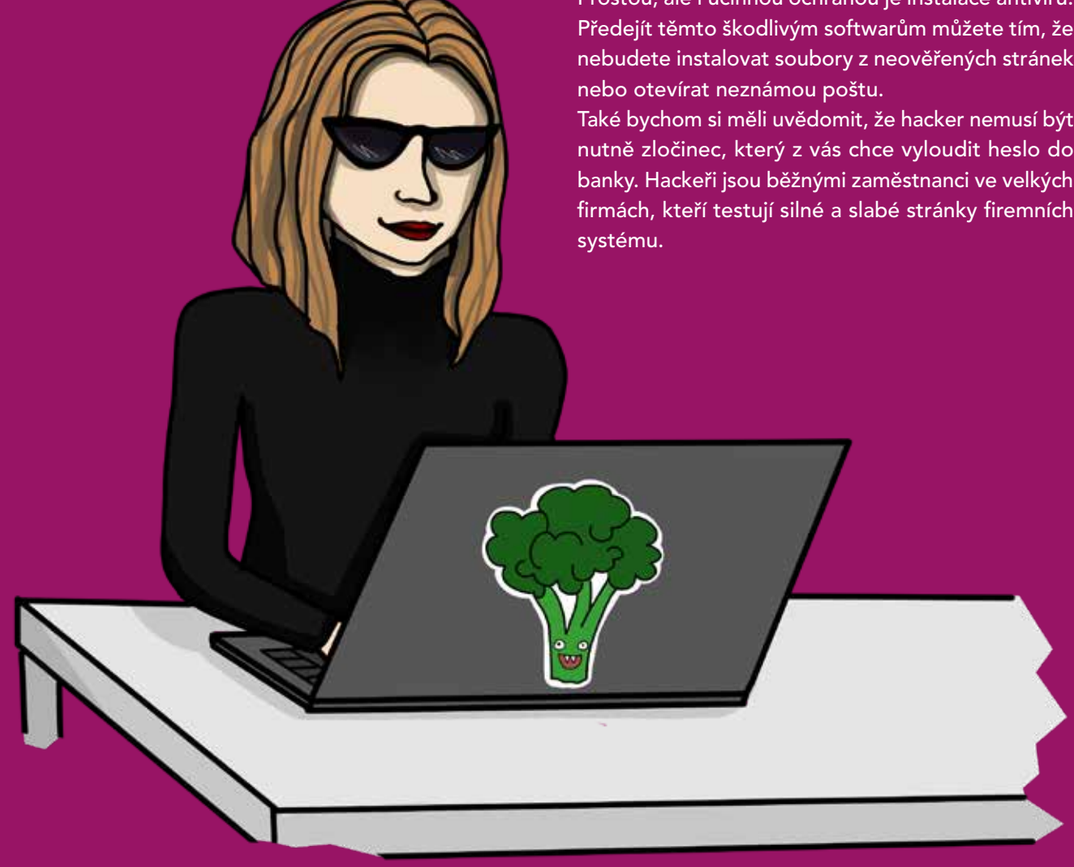


V současné době se na internetu můžete sektat s velkou spoustou hrozeb, které na vás číhají i při obyčejném používání internetu. Ty nejčastější a nejnebezpečnější jsme se pro vás pokusili shrnout na následujících stranách a přiblížit co vše se vám může stát a jak postupovat, když se ocitnete v potížích.

HACKERSKÉ TECHNIKY

Hackera si určitě velká skupina lidí představuje jako člověka, který sedí před obrazovkou, na které se chaoticky míhají dialogová okna, zběsile mlátí do klávesnice a díky tomu se dostává do tajných serverů nebo do bank. To je většinou představa, kterou nás krmí akční filmy a mi ji nějak blíže nezkoumáme.

Pravdou je, že hackeři mohou zaútočit i na váš počítač. Opravdu jejich cílem nemusí být jen obrovské korporace, výdělečné společnosti nebo vládní servery. Ani nemusí mít nějaký určitý důvod, náhodou rozkliknete přílohu u pochybného e-mailu, nebo si stáhnete zavirovaný soubor.
Hackeři pracují za pomoci skriptů nebo programů, které manipulují s přenášenými daty. Je spoustu hackerských technik a jednou z nich je používání malware. Malware neboli „škodlivý software“ je tajný přístup do vašeho zařízení. Ten si většinou stáhnete s filmem, hudbou nebo hrou, aniž byste o tom věděli.



Maleware má více typů:
Nejznámějším je nejspíše virus. Ten funguje tak, že postupně získává kontrolu nad vaším zařízením a provádí různé destruktivní akce a změny.
Dalším velmi „slavným“ malewarem je Trojský kůň. Ten se stejně jako ten skutečný tváří jako užitečná funkce nebo zábavná hra, která však ve skutečnosti způsobuje škody nebo krádeže dat.
Velmi nepříjemný pro váš počítač může být i počítačový červ, který se postupně sám množí, až zahltí vaše zařízení tak, že přestává reagovat.
Pokud jde o výzvědné softwary, spyware je právě jedním z nich. Je velmi obtížně odhalitelný a skrytě sbírá informace o vašem chování na internetu, vaší historii prohlížení stránek nebo vaše hesla a osobní údaje.
Napadené zařízení sice neprokazuje nějaké do očí bijící znamení v podobě kódu z Matrixu nebo dramatického rozzrnění obrazovky, jako tomu často bývá v televizi, ale i tak je ve většině případů snadno odhalitelné. Počítač začíná pomaleji reagovat na vaše příkazy, celkově se přehřívá, nebo se objevují problémy s připojením k internetu. Dále se můžou začít objevovat neznámé soubory nebo aplikace, které jste si sami nenainstalovali.
Prostou, ale i účinnou ochranou je instalace antiviru. Předejít těmto škodlivým softwarům můžete tím, že nebudete instalovat soubory z neověřených stránek nebo otevírat neznámou poštu.
Také bychom si měli uvědomit, že hacker nemusí být nutně zločinec, který z vás chce vyloudit heslo do banky. Hackeři jsou běžnými zaměstnanci ve velkých firmách, kteří testují silné a slabé stránky firemních systému.

PHISHING
INTERNETOVÉ RHYBAŘENÍ

Určitě už se to každému někdy stalo, přijde vám e-mail většinou z vašeho internetového bankovnictví, a odesilatel, tedy podle vás vaše banka, vám oznamuje, že je s vaším bankovnictvím něco v nepořádku, a pro co nejrychlejší vyřešení máte v dopise odkaz na přihlašovací doménu. Rychle rozkliknete a před vašima očima vidíte naprosto stejné prostředí pro přihlášení jako vždy. Nic vás nezarazí. Vyplníte své jméno a poté heslo. Jenže místo přihlášení do bankovnictví poskytnete svoje přihlašovací údaje útočníkům, kteří teď mají možnost obrat vás o peníze. Jste chyceni…

Phishing se na internetu vyskytuje již pěknou řádku let. Už v druhé polovině devadesátých let se jeho obětí stal poskytovatel internetových služeb AOL. Zákazníkům této firmy začali chodit „ověřovací e-maily," které je žádali o vyplnění citlivých údajů. Phishing začal být tak častý, že AOL do všech zpráv přidával řádek o tom, že se žádný jejich pracovník neptá klienta na heslo, ani na údaje o účtu.

Od té doby se ale rhybaření rozrostlo do neuvěřitelných rozměrů. Útočníci se převážně zaměřují na zákazníky online bank. Zatímco dříve byly rozesílány zprávy náhodně a útočníci čistě jen doufali, že e-mail s určitou bankou dorazí některým z jejích zákazníků, dnes se častěji setkáme s tzv. spear phishingem. Při tom jsou rhybáři schopni rozpoznat, jakou banku používáte, a poslat vám tedy příslušný e-mail.
A je vůbec nějaký způsob ochrany? Je spoustu bodů, které lze poznat na podvodném e-mailu. Například rovnou v textu. Pokud je celý napsán v jiném jazyce než obvykle, je napsán s gramatickými chybami nebo mu třeba chybí diakritika, jedná se o podvod.
Jestli je text napsán správně, při rozkliknutí odkazu bychom měli zjistit, jestli je stránka zabezpečená, tedy jestli je v odkazu na horní liště uvedeno https včetně „s" a jestli je celkový odkaz napsán správně.
Ale stále nejjednodušší a nejúčinnější je neklikat na přiložené odkazy. Prostě si otevřít příslušnou stránku, například internetové bankovnictví ručně přes nové okno a předejít tak chycení.

KYBERŠIKANA

Vyrůstat v době, kdy se moderní technologie staly naší součástí, přináší nové, často nepříjemné zkušenosti. Obtěžování přes komunikační prostředky, krádeže identit, vydírání,… s tím vším se může uživatel ve virtuálním světě setkat. Jedná se o činnosti, které patří pod kyberšikanu.

Virtuální svět je rouška, pod kterou se může ukrýt kdokoliv a být kýmkoliv. Anonymita, která nás má chránit, se stává krycím prostředkem pro agresory, aby dosáhli svého cíle – napadení oběti.
Agresoři, kteří se dopouští kyberšikany, ohrožují psychické zdraví své oběti. Jejich útok se může lišit. Někteří dávají přednost psaním urážlivých zpráv nebo pořizování zesměšňujícího materiálu, jiní se dopouštějí vydírání, které je často spojené s pořizováním erotických záznamů oběti. Agresor se v těchto případech dopouští trestného činu. Oběť se nesmí bát zakročit a jestli to dojde do kritického stádia, měla by to i nahlásit případným orgánům.

Kyberšikana je vážná věc, proto bychom měli dělat opatření, jak jí předejít.
Základním pravidlem by mělo být, že si mezi své přátele na sociálních sítí nebudeme přidávat někoho, koho neznáme nebo si přinejmenším prohlédneme profil člověka, který se s námi chce seznámit. Jestli v jeho přátelích najdeme naše známé, může nás to ujistit, že se nejedná o falešný účet. Tahle metoda ovšem není stoprocentní.
Měli bychom omezit šíření soukromých informací. Bydliště, datum narození nebo číslo bankovního účtu jsou důležité údaje pro nás, ne pro celý svět.
Se soukromým také souvisí fotografie a videa, která sdílíme s veřejností či s vybranou osobou. Vždy bychom se měli vyvarovat zasílání citlivého materiálu. Fotka, kterou tak můžeme sdílet jenom s jednou osobou, může další den vidět celý svět, jelikož agresor nerespektoval naše soukromí.

Ačkoliv se šikana ve virtuálním světě může zdát neškodná, neměli bychom ji brát na lehkou váhu. Jestli se v našem okolí nachází osoba ohrožená tímto typem násilí, měli bychom se snažit jí pomoci.
Nejlepší způsob je agresora zablokovat na úplném počátku, tím předejdeme veškerým potížím.

ZABEZPEČENÍ

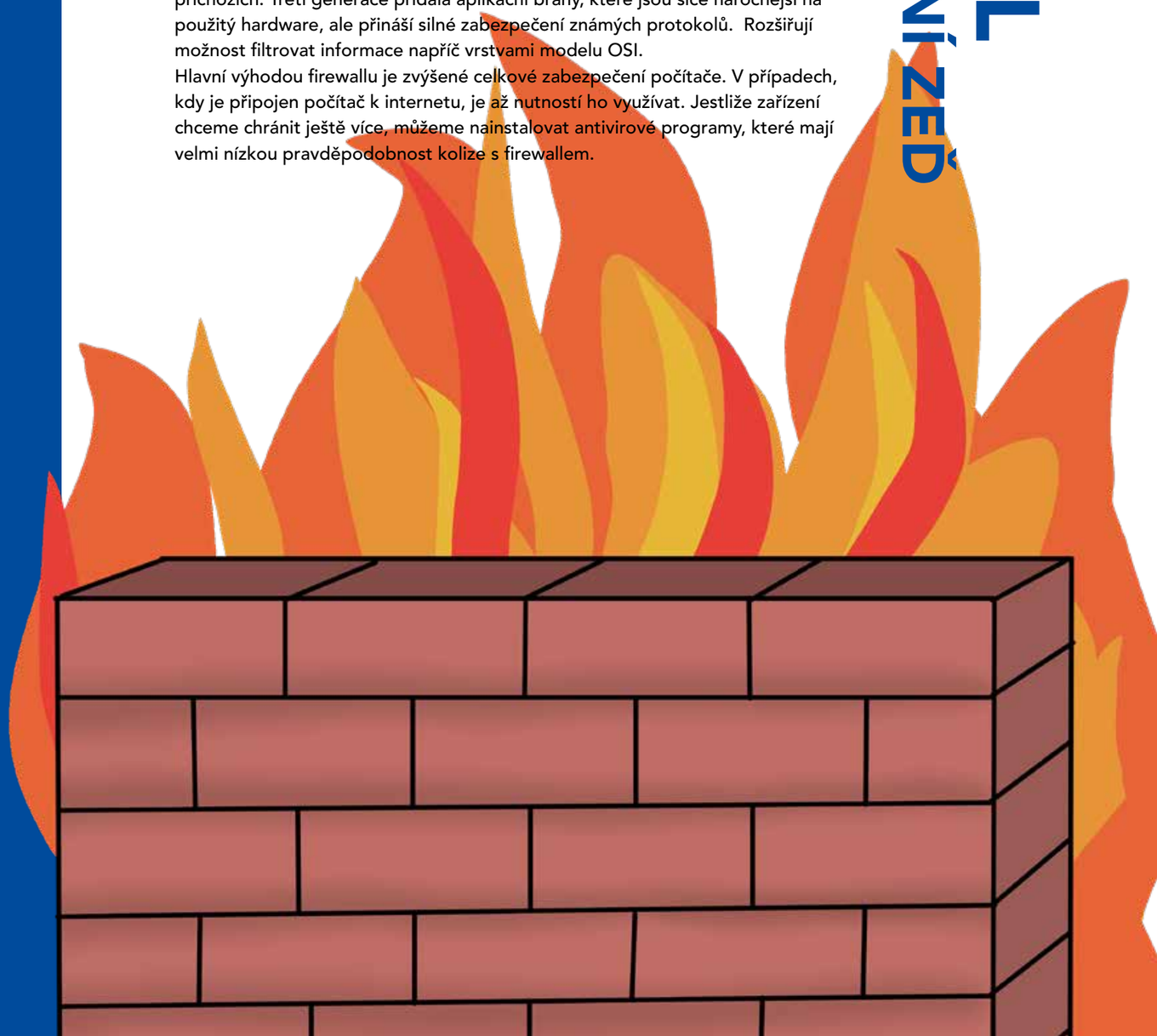
Na následujících stranách se vám pokusíme přiblížit jaké existují druhy zabezpečení vašich zařízení, jak předejít nechtěné ztrátě dat nebo nevítané návštevy ve vašem počítači. Zasvětíme vás do světa antiviru a představíme vám, co je to Firewall, a jak pracuje.

FIREWALL

PROTIPOŽÁRNÍ ZEĎ

Svět je nebezpečné místo, a to samé platí i s počítačovými sítěmi. Způsobů, jak se chránit ve světě není mnoho, ale pro počítačové sítě to neplatí. Jedním ze způsobů, jak předejít potížím zapříčiněným nechráněným přenosem dat mezi počítačem a internetem, je firewall.

Hlavní úloha firewallu je rozhodnout dle předdefinovaných pravidel, jak bude nakládat s příchozími a odeslanými komunikacemi, jestli je pustí dovnitř nebo ven. Můžeme si to představit jako ochranku, která střeží vstup nebo jako polopropustnou zeď.
Firewall se vyvíjel od konce minulého století. První generace využívala paketové filtry, které sledují síťové adresy a porty paketu, aby rozhodly, jestli má být tento paket povolen nebo zablokován. Druhá generace, která se přesunula na stavové filtry, umožňovala rozeznat pakety, které byly již povolené od nově příchozích. Třetí generace přidala aplikační brány, které jsou sice náročnější na použitý hardware, ale přináší silné zabezpečení známých protokolů. Rozšiřují možnost filtrovat informace napříč vrstvami modelu OSI.
Hlavní výhodou firewallu je zvýšené celkové zabezpečení počítače. V případech, kdy je připojen počítač k internetu, je až nutností ho využívat. Jestliže zařízení chceme chránit ještě více, můžeme nainstalovat antivirové programy, které mají velmi nízkou pravděpodobnost kolize s firewallem.



JAK SPRÁVNĚ ZABEZPEČIT POČÍTAČ

Jestli hledáte nějaké tipy, jak zabezpečit svůj počítač před nečekaným pádem nebo loupeží, tak to hledáte marně. Přesto doporučuji dočíst dokonce. Počítač je totiž důležité chránit hlavně zevnitř.

1.

Jako první bych zmínila věc, která už je vám známá. Nevěřit e-mailům a v žádném případě neklikat na odkazy a neotvírat přílohy od neznámých odesílatelů. Takový e-mail vám může do počítače nainstalovat program pro vzdálený přístup k počítači. A pak se můžou stát věci, které byste nechtěli.

2.

Už jste určitě u někoho viděli přelepenou webovou kameru. Jestliže se pak totiž někdo naboural do vašeho počítače, díky web kameře vás potom někdo může sledovat. A co hůř natáčet a následně vydírat. Proto naše rada zní - pozor na web kamery.

3.

Pak jsou tady emaily, které požadují přihlášení na nějakou webovou stránku, kde jsou vaše osobní údaje, či přihlášení k bankovnímu učtu. Rozhodně nic nevyplňujte. Do emailu vůbec nepatří osobní citlivé informace, číslo kreditní karty či různá hesla. A to ani do nevyžádané pošty, ani do emailů někomu známému.

4.

Co se uživatelských účtů týče, je nutné mít silné a ne snadno uhodnutelné heslo. Uvádí se, že optimální heslo by mělo obsahovat okolo 10 znaků. Některé stránky vyžadují kombinaci velkých a malých písmen a číslic. Než si ale vymyslíte změť písmenek a číslic, položte si otázku, zda si takové heslo budete pamatovat. Ptáte se, zda mít na každý účet nové heslo? Mít několik desítek hesel je trochu přehnané, na druhou stranu mít jen jedno heslo na všechno, je dost troufalé.

5.

Další důležitou věcí je mít nainstalovaný nějaký antivirový program, který budete pravidelně aktualizovat. To si ale zaslouží svůj vlastní článek.

6.

„Už to zase chce novou aktualizaci!“ Věta, kterou aspoň jednou použil každý z nás. Aktualizace operačního systému je ale velmi důležitá. Nejen že opravuje chyby, malé skulinky, přes které by se útočníci a viry mohly do počítače dostat, ale aktuální systém chrání a upozorňuje před případnými potížemi.

Všechny tyto rady neplatí ale jen pro vaše počítače. Tablety a telefony je třeba také chránit. Proto pravidelně aktualizujte software a zvažte stáhnutí nějakého antiviru.

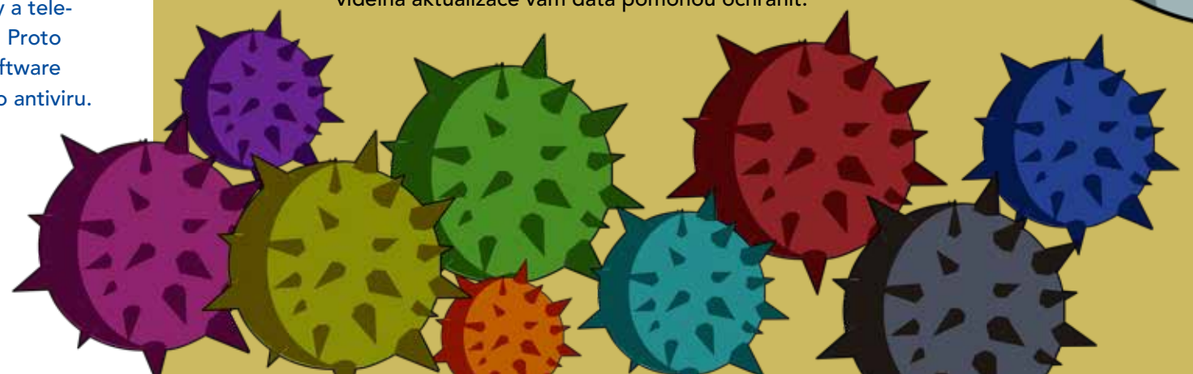
ANTIVIR

Abychom navázali na předchozí článek, antivirové programy jsou jedni z nejúčinnějších zabezpečení Vašeho počítače. Jedná se o počítačový software, který nejenže odstraňuje počítačové viry, ale dokonce je dokáže snadno eliminovat. Samozřejmě, že operační systém vašeho počítače obsahuje nějakou antivirovou ochranu, proto je velmi dobré a doporučuje se si tuto ochranu vylepšit.

Jak už víme, phishing je jedna z nejčastějších technik roznášení počítačových virů. Jedním z nich je Počítačový červ, který jakmile napadne počítač, začne prolézat internetem a bez vědomí uživatele rozesílat viry do dalších počítačů. Nebo například vir Trojský kůň. Nepleťme si ho s velkým dřevěným Trójským koněm. Tento vir vypadá jako užitečný program, ale stejně jako Trójský kůň dokáže počítači otevřít „zadní vrátka“ a proniknout do něj.
Existuje celá řada virů a programů, které nám viry do počítače instalují. Některé dokáže zachytit a upozornit vás na ně váš počítačový software. Některé viry obsažené v různých nepříjemných programech však potřebují účinnější ochranu, kterou vám antivir může poskytnout. Samozřejmě jsou tady ještě různá důležitá opatření, jako je například bezpečné heslo, ale to už jsme si vysvětlili.
Tím, že si jen stáhnete nějakou antivirovou aplikaci, si bezpečí nezabezpečíte. Velmi důležité jsou aktualizace - a to jak počítačového softwaru, tak samotné antivirové aplikace.

Jestliže nevěříte bezplatným programům, ale peníze se vám za to dávat nechtějí - nebojte se. Tvůrci vydělávají především na reklamách, které se v bezpečnostních programech zobrazují. Na druhou stranu, máte-li ve svém počítači velmi důležité a soukromé věci, placená lepší nebo plná verze aplikace pro vás bude bezpečnější.
Mezi nejznámější bezplatnou ochranu v naší republice patří nejspíše aplikace **Avast Free Antivirus**. Hledat a odstraňovat viry můžete přímo z programu, lepší je ale možnost automatického prohledávání a hlídání bezpečnostního systému. Program sám během vaší běžné práce na počítači bude hlídat případné viry. Navíc program skvěle funguje i na starších, méně výkonnějších počítačích. Dalšími možnými antivirovými programy jsou například **Ad-Aware, Eset, Zonealarm, AVG**,…

Mít všechna svá potřebná data a údaje na papíru a nosit štosy takových papírů všude s sebou přeci není nejpříjemnější. Nebojte se mít všechna svá data v přenosném počítači nebo jiném zařízení, které bude mnohem lehčí a šikovnější na hledání než štosy papírů. Vhodný antivirový program a pravidelná aktualizace vám data pomohou ochránit.

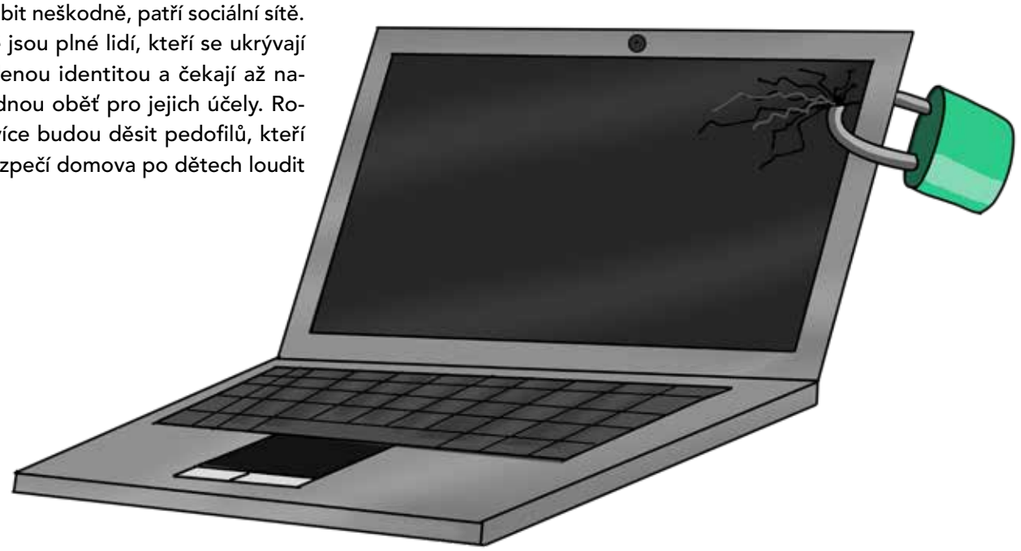


ONLÍNE

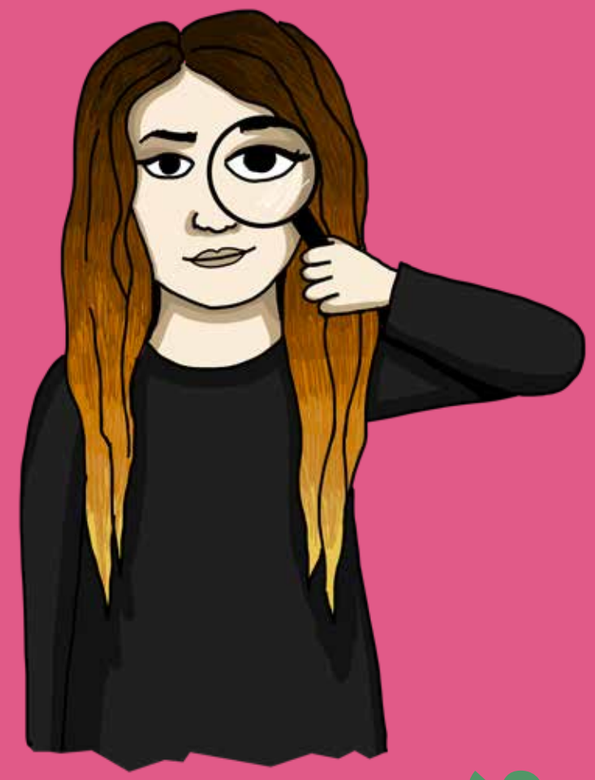
Děti chodící po ulici se skloněnou hlavou, ozářeným obličejem a nevěnující pozornost svému okolí, není dystopická budoucnost, ale moderní doba. Rodiče pomalu vzdávají boj, aby svým dětem zakázali užívání moderních technologií. Děti tak dostávají příležitost prozkoumávat „nový svět," který má nekonečné možnosti. Rodiče by se měli snažit i na internetu, dítě co nejvíce chránit, a proto by mu měli vytvořit bezpečné online prostředí, ve kterém se bude nacházet.

Základem je, aby dospělá osoba, která má nad dítětem dohled, ovládala a průběžně se vzdělávala v online prostředí.
Existuje nesčetné množství nebezpečných stránek pro děti. Mezi jedny z těch nejnebezpečnějších stránek, které na první pohled můžou působit neškodně, patří sociální sítě. Sociální sítě jsou plné lidí, kteří se ukrývají pod vymyšlenou identitou a čekají až naleznou vhodnou oběť pro jejich účely. Rodiče se nejvíce budou děsit pedofilů, kteří mohou z bezpečí domova po dětech loudit pornografický obsah. To ovšem nejsou jediní útočníci na sociálních sítích. Dítě se tam může setkat s kyberšikanou, člověkem, který po něm bude chtít peníze či nějakým násilníkem, který může dítě vylákat na veřejné setkání, ze kterého se dítě už nemusí vrátit. Nejvhodnějším způsobem, jak dítě na internetu chránit, je využívat aplikace tzv. rodičovské filtry a zámky, jež zablokují stránky dle našich požadavků. Naneštěstí tyto aplikace nedokáží zabránit úplnému zabezpečení dítěte, jelikož nové nepatřičné stránky vznikají každý den, přesto můžou silně omezit přístup k nevhodnému obsahu. Jako bonus jsou tyto aplikace často vybaveny i sledováním polohy zvoleného zařízení.
Mezi další způsoby ochrany patří vzdělávací dokumenty s tématikou bezpečnosti na internetu, které můžeme dítěti pustit, aby bylo poučeno o správném chování. Ovšem nejlepší cestou, jak dítě chránit je s ním komunikovat. Jestliže zaznamenáme podezřelé chování, mělo by se to urychleně řešit, aby to nemělo fatální důsledky.

ONLINE BEZPEČÍ



HTTP, HTTPS, WWW, hypertext a mnoho dalších! To všechno jsou zkratky, které známe a pravidelně používáme. Kolik lidí ale zná přesnou definici a význam těchto zkratek? Pokusím se vám pojmy přiblížit a vysvětlit vám, proč je tak důležité si takových to zkratek všímat.



HTTP je zkratka pro Hypertext Transfer Protokol, což vlastně znamená protokol přenosu hypertextů. Abychom si vysvětlili pojem hypertext - jedná se o odkazy na rozšíření informací. Kliknutím na hypertextový odkaz se dostaneme na stránku, která nám poskytne více informací o vybraném slově. Myslím si, že to ale známe každý. Krásným příkladem je online encyklopedie Wikipedie. V každém článku a v každém odstavci je spousta modrých slov - hypertextových odkazů, které nás přenesou na novou, více informovanou stránku. Více informací dostaneme ale o slovu, které jsme rozklikli.

HTML je internetový protokol, který je určený hlavně pro komunikaci s WWW servery. WWW, web neboli World Wide Web v překladu celosvětová síť. Systém prohlížení, ukládání a odkazování dokumentů v internetu. Těmto dokumentům říkáme webové stránky. Pomocí hypertextových odkazů jsou na webových serverech uloženy webové prohlížeče, přes které si prohlížíme zmiňované webové stránky. Dle mého názoru to pro laiky může být matoucí, proto si z toho pojďme vyvodit závěr. Celá tahle webová pavučina je přenesena HTTP protokolem. A jelikož, stejně jako svět reálný obsahuje ten webový spoustu virů, je důležité dívat se jen na stránky zabezpečené.
Na rovinu, samotné HTTP není chráněné před odposloucháváním, sledováním či modifikací obsahu. Návštěvník si ani nemusí všimnout, že ho někdo může „sledovat." Nezabezpečené HTTP také nezaručuje, že obsah, který se dostane do prohlížeče, je ten obsah, který vytvořila příslušná webová stránka. Například i po připojení neznámé Wi-Fi síti může její poskytovatel sledovat připojené uživatele.

Pro zabezpečení HTTP se používá spojení, které se následně stane HTTPS. Co znamená HTTPS? Úplně to samé co HTTP, akorát zabezpečené a bezpečnější. Někteří moc rozdílů mezi HTTP a HTTPS nevidí, ovšem jeho používání je mnohými odborníky doporučeno. HTTPS totiž představuje účinnou obranu proti vkládání obsahu, o který nestojíme - například nevyžádané reklamy. V HTTPS také máme důvěrnost přenášení dat a cizí návštěvníci nás jen tak a snadno nemohou sledovat.
Je důležité si dávat pozor na výběr správné stránky tak, abychom omylem neotevřeli dveře nezvaným hostům. Proto až dnes budete brouzdat internetem, zkuste se podívat, zda je v „hlavičce" HTTP nebo HTTPS. Nejpoužívanější stránky HTTPS obsahují a v této době se málokdy setkáme jen s HTTP. Když už ale na nějaké takové stránce budete, nezdržujte se tam moc dlouho a dveře cizím návštěvníkům zavřete dřív, než jimi stihnou proklouznout.

HTTP A HTTPS

ONLINE NAKUPOVÁNÍ

Spěcháte, musíte do obchodu pro jednu věc, kvůli které strávíte na místě zbytečně mnoho času, jelikož fronty neberou konce, nebo potřebný předmět nemůžete nalézt a místo něj zakoupíte zbytečnosti, které vás zaujaly během hledání, zní vám to povědomě? Jako řešení se ve světě rozšířilo nakupování na internetu.

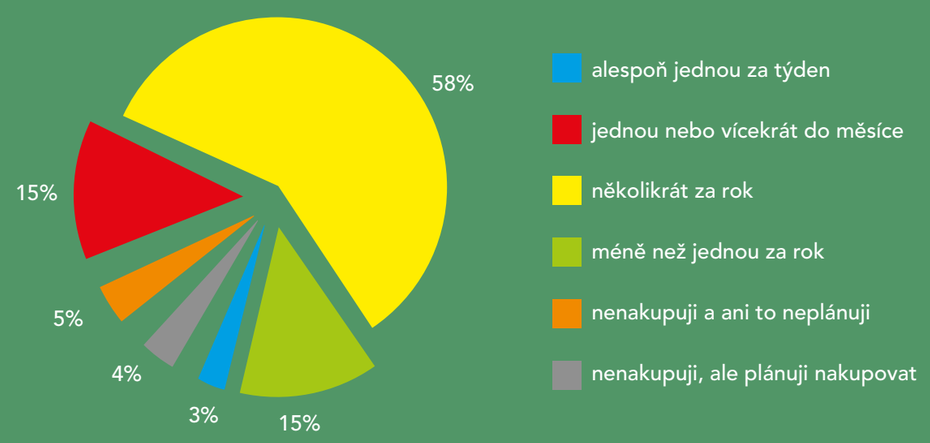
Nákup potravin v obchodě, který se stával obvyklým rodinným výletem, je minulostí. Stačí na moment sednout k počítači a vše je zařízeno. Na co bychom si však při nakupování přes internet měli dát pozor?

Online nakupování by se dalo rozdělit do tří důležitých fází. První by byla správná volba webové stránky, ze které výrobky chceme odkoupit. Zde platí, že bychom měli dát na první dojem, jestliže se nám prostředí a vzhled stránky bude zdát neprofesionální nebo na začátku internetové adresy bude scházet "https", raději bychom měli zvolit jinou.
Také bychom se měli vyhýbat obchodům, které nabízí až nesmyslně nízké ceny. Jedná se většinou o virtuální tržiště, jejichž prodejci často pocházejí z Číny. Kvalita zboží zde bohužel odpovídá ceně.
Druhou fází je poté samotné objednání. Vyplníme vše důležité, co se dodání týče, a poté volíme platbu.
Pokud nechcete nesmyslně přeplácet za dobírku, je zde několik možností. Kromě platby kartou existují i digitální peněženky jako například PayPal nebo české GoPay.
Tyto peněženky fungují na různých systémech. Některé jsou propojeny s vaším účtem, prostřednictvím kterého čerpají finance na platbu. Jiné musíte před použitím penězi „dobít.“ Můžeme ale najít i takové, které oba principy slučují.

Poslední fází je poté samotné dodání. Zde bychom si měli zkontrolovat stav objednávky. Poškozené zboží odmítnout a nechat ho poslat zpět. Jestliže zásilka nepřijde do stanoveného data, snažíme se domluvit s prodejcem na vhodném řešení.

Internetové nakupování je uzpůsobeno všem, je jednoduché a dostupné, proto bychom se mu neměli bránit.

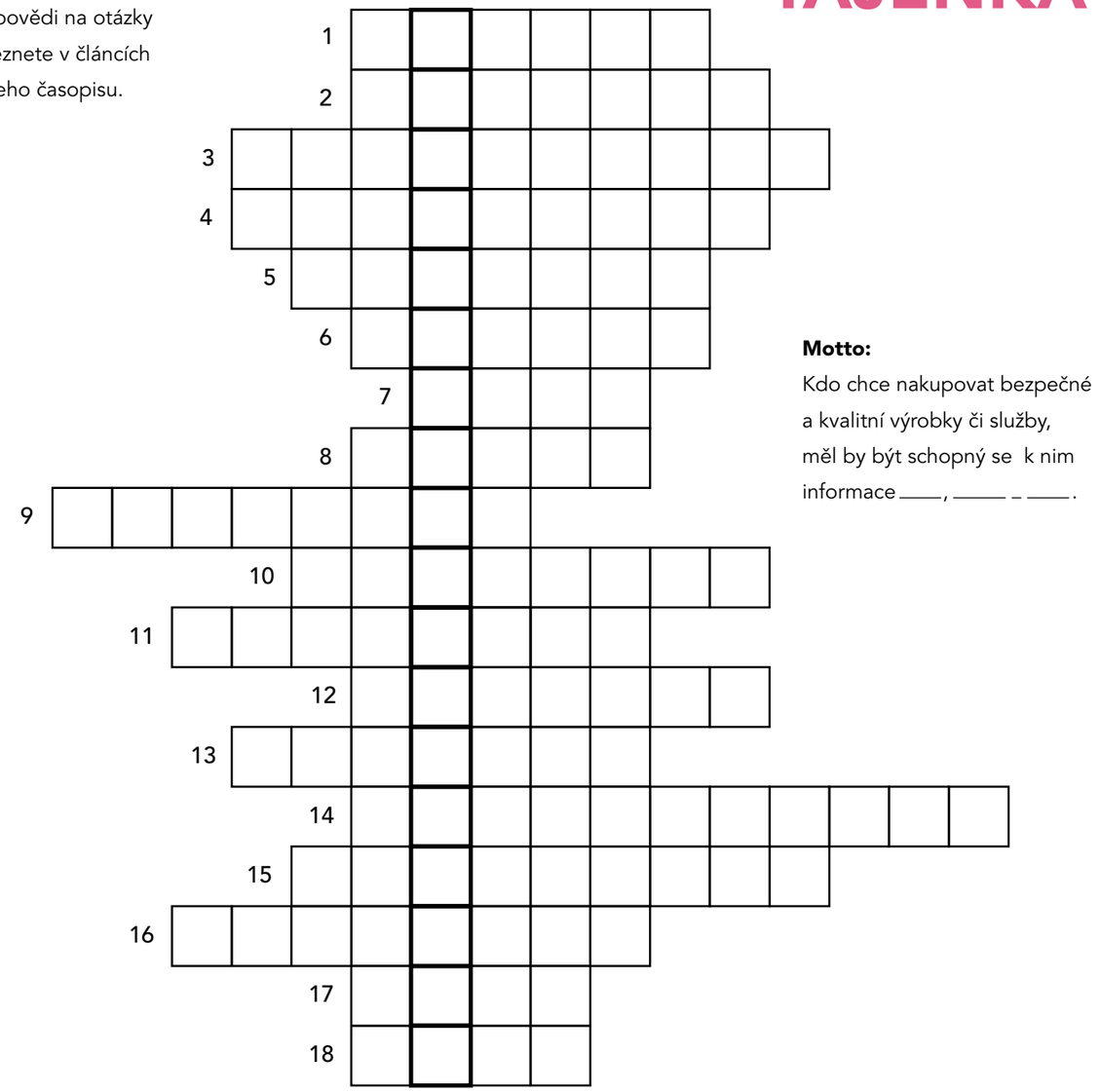
Jak často nakupujete prostřednictvím internetu?



Průzkum provaedla agentura Mediaresearch pro internetový obchod Alza.cz.

TAJENKA

Odpovědi na otázky naleznete v článcích našeho časopisu.



Motto:
Kdo chce nakupovat bezpečné a kvalitní výrobky či služby, měl by být schopný se k nim informace ____, _____ _ ____.

1. Děkujeme, že čtete náš časopis .....
2. Jak se nazývá škodlivý obsah, díky kterému mohou hackeři do našeho počítače?
3. Nejslavnější škodlivý obsah.
4. Firewall, je nechráněný přenos dat mezi internetem a .....?
5. Do e-mailů od neznámých odesílatelů nikdy nevyplňuji ..... údaje.
6. E-mail s gramatickými chybami je?
7. Phishing je nejčastější technika roznášení počítačových ....?
8. Rodiče by měli ....., co dělají na internetu jejich děti.
9. Ti, kteří se dopouštějí kyberšikany se nazývají?
10. Internetové rhybaření.
11. První generace před vyvinutím Firewallu využívali ..... filtry.
12. Kolik procent lidí nakupuje na internetu pravidelně alespoň jednou za měsíc?
13. HTML, je protokol určený pro komunikaci s WWW ....
14. Jak se nazývá obtěžování, vydírání či krádeže identity ve virtuálním světě?
15. Šíření jakých informací bychom měli na internetu omezit?
16. Aktualizace operačního systému je velmi .....?
17. Jedny z nejnebezpečnějších stránek mohou být sociální ....
18. Jakou zkratku má protokol pro přenos hypertextů?

Informace jsme čerpaly zde:

https://cs.wikipedia.org

http://ppk.chip.cz

https://www.eset.com

https://jecas.cz

https://blog.avast.com

https://www.e-bezpeci.cz

https://www.novinky.cz/internet-a-pc

https://www.antivirovecentrum.cz

https://www.alza.cz/

OnLine
V době digitální…

květen 2020

redakce:
Barbora Popielová
Tereza Stehlíková
Tereza Trnková

Obchodní Akademie
České Budějovice
Husova 1

www.oacb.cz