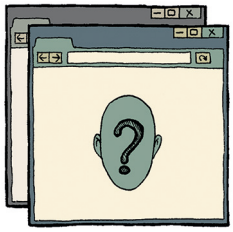
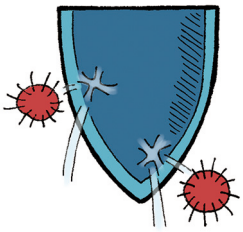
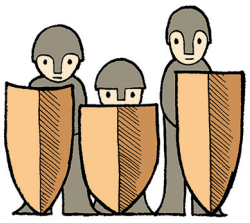


Anonymní okno



Antivir

CAPTCHA

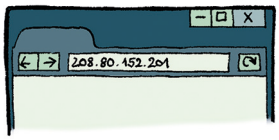


CSIRT

Digitální stopa

Grooming

Hacker

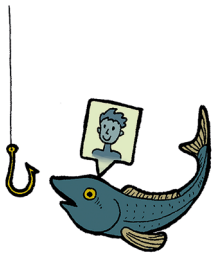


IP adresa

Kyberšikana

Nomofobie

Záplata



Phishing

Pirátství

Ransomware

Router

Řetězový dopis

Pexeso

Počet hráčů: 2 a více
Věk hráčů: 3–99 let

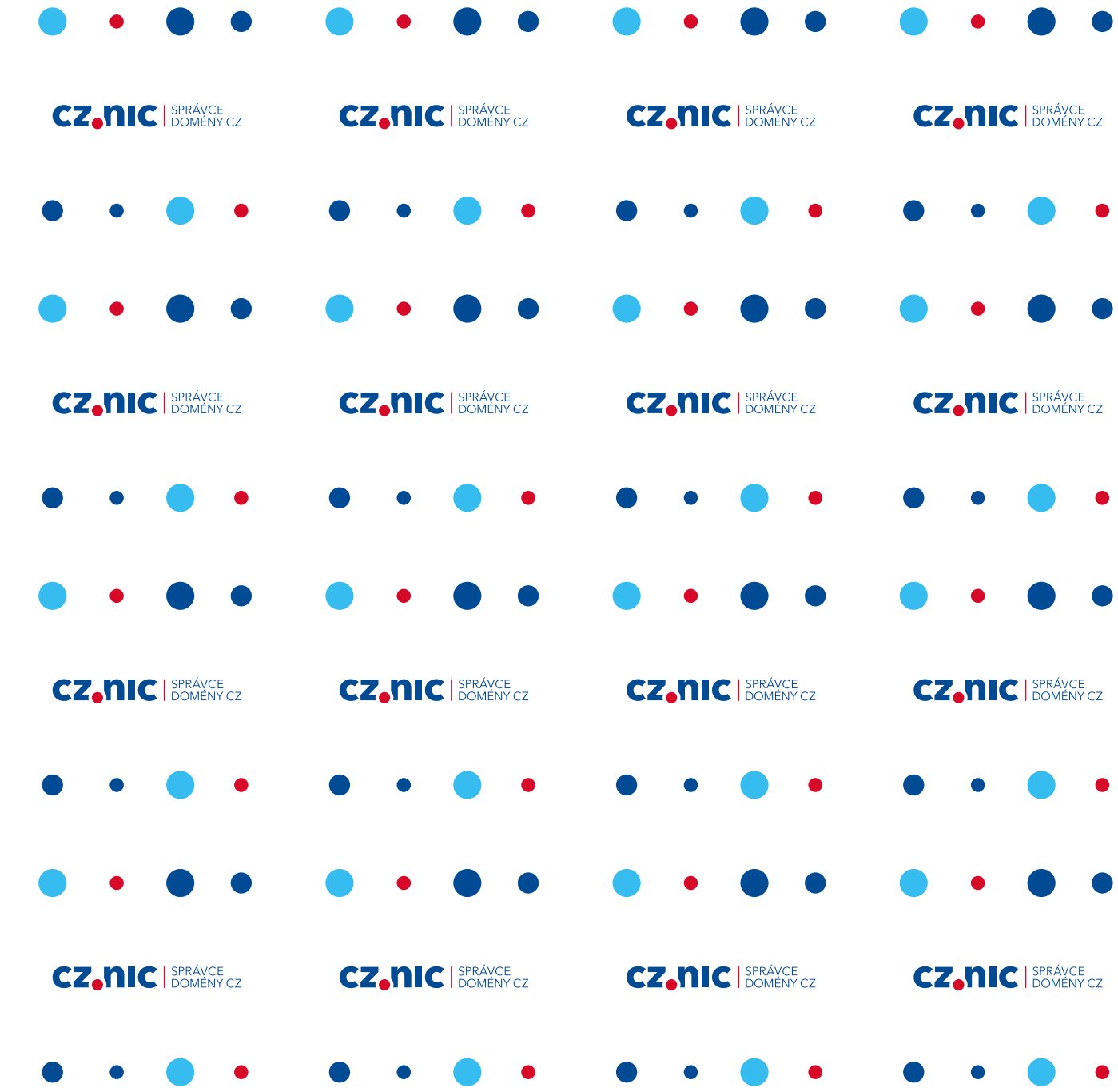
2 × 🖨 → ✂
Tisk: oboustranný (duplex)
Měřítko: skutečná velikost (100 %)

Pravidla hry:
Karty se zamíchají a rozloží lícem dolů tak, aby žádný z hráčů neznal rozložení karet. Hráči postupně otáčí dvojici karet lícem vzhůru, aby je viděli i ostatní hráči. Pokud karty patří k sobě, hráč je odebere a otáčí další dvojici. Pokud karty k sobě nepatří, otočí je zpět lícem dolů a pokračuje další hráč v pořadí. Hraje se tak dlouho, dokud nejsou všechny karty rozebrány. Vítězem se stane hráč s největším počtem nalezených dvojic.

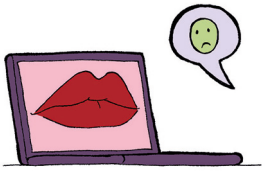
CZ.NIC | SPRÁVCE DOMÉNY CZ

BEZPEČNĚ NA NETU

Spolufinancováno Evropskou unií
Nástroj pro propojení Evropy



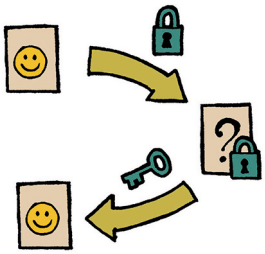
Sdílení



Sexting

Soukromí

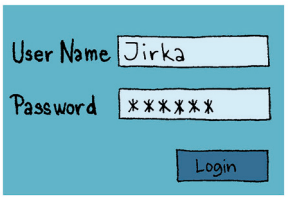
SPAM



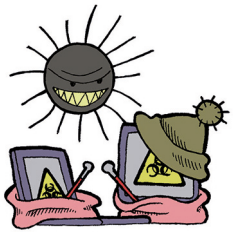
Šifrování

Trojský kůň

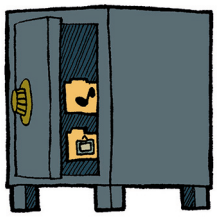
Útok



Uživatelské jméno/heslo



Virus



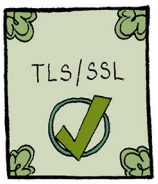
Zálohování

Zombie

DNSSEC

Honeypot

Kybernetická kriminalita



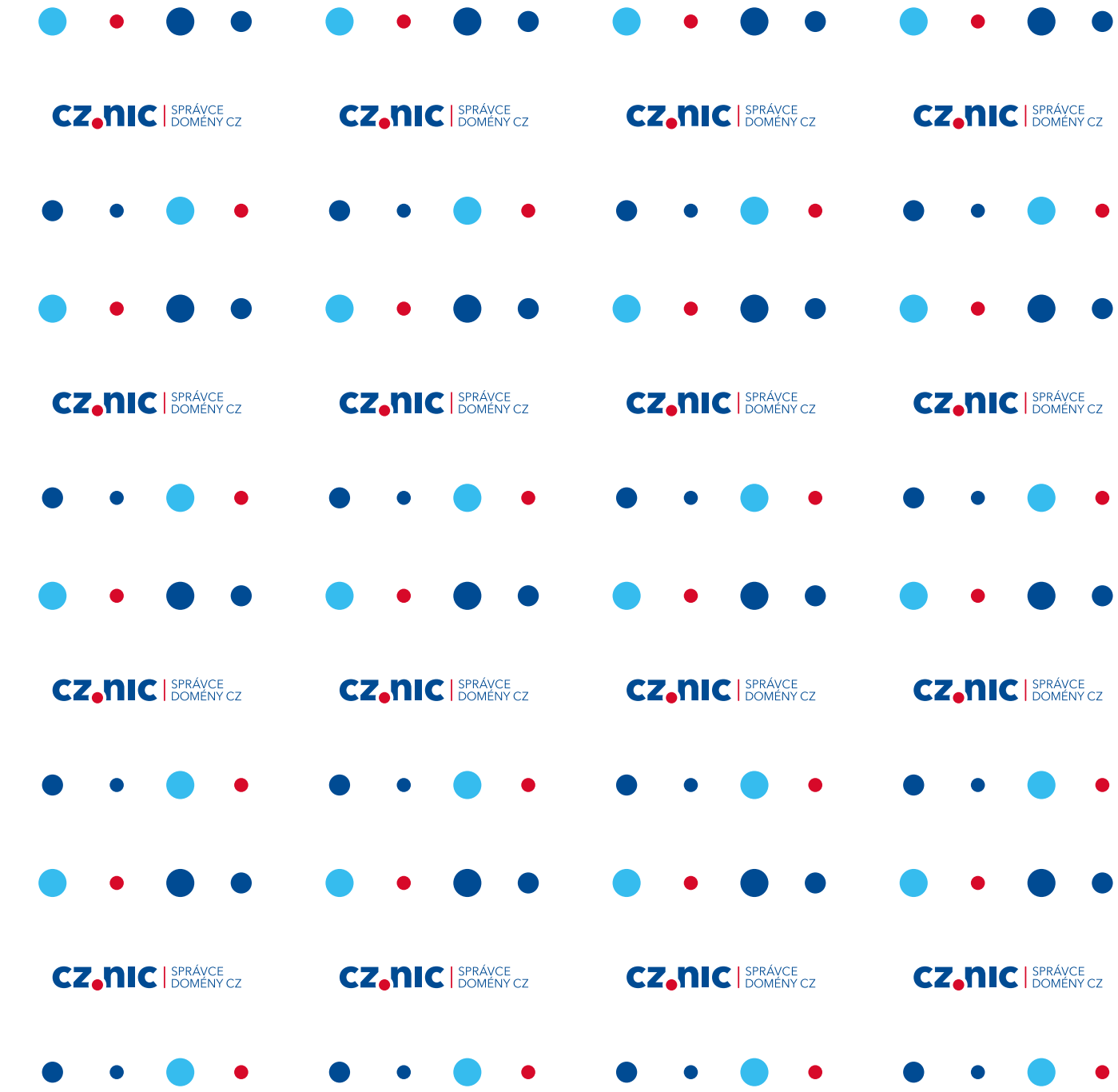
TLS/SSL certifikát

Wi-Fi

CZ.NIC | SPRÁVCE DOMÉNY CZ

BEZPEČNĚ NA NETU

Spolufinancováno Evropskou unií
Nástroj pro propojení Evropy



Anonymní okno

Možnost nastavit internetový prohlížeč tak, aby neukládal informace o tom, co na Internetu děláte. Pokud například chcete rodičům tajně koupit dárek k narozeninám a bojíte se, aby nebyl prozrazen prostřednictvím reklamy, která vyskakuje po vyhledávání zboží, stačí v pravém horním rohu prohlížeče kliknout na tři čárky, nebo tečky (záleží, jaký prohlížeč využíváte) a zvolit možnost „Anonymní okno". Lze také využít klávesové zkratky Ctrl + Shift + N pro Google Chrome a Opera a Ctrl + Shift + P pro Internet Explorer a Mozilla Firefox.

Antivirový program

Počítačový program, který funguje podobně, jako když se rodiče snaží předejít našemu nachlazení. Mohou to dělat dvěma způsoby. Ve chvíli, kdy kašleme, nás vezmou k doktorovi, aby zjistil, zda již v sobě náhodou nemáme nějaký bacil. Druhý způsob je ten, že když vědí, že je kamarád nemocný, nepustí nás si s ním hrát, abychom se nenakazili. Podobně fungují i antivirové programy. Kontrolují, jestli vše, co je v našem počítači, je zdravé a snaží se zabránit tomu, aby náš počítač chytil nějakou infekci od jiného již nemocného zdroje, například nějaké hry, kterou se chystáme stahovat.

CAPTCHA

Hackeři dokážou vytvářet kódy, které umí samy zkoušet různé kombinace hesel. Těmto kódům se říká roboti. Roboti mají proti člověku spoustu výhod, ale jednu velkou nevýhodu. Neumí poznat jiná než perfektně napsaná písmenka. A taky nevědí, jak ve skutečnosti vypadá strom, květina nebo zvířátko. Člověk ví, že B je pořád B, i když mu chybí kousek spodního bříška nebo je napsáno nakřivo, pozná, na kterém obrázku je příroda nebo zvířátko, ale roboti tuto vlastnost zatím nemají. Využíváním CAPTCHA tedy majitelé různých webů brání své uživatele před krádeží jejich účtů nebo sami sebe před přívalem nevyžádané pošty.

CSIRT

CSIRT je zkratka písmenek týmu, který se stará o bezpečnost podobně jako policisté. Rozdíl je v tom, že členové CSIRT týmů se starají o bezpečnost v kyberprostoru, tedy všude tam, kde jsou počítače nebo servery připojené k Internetu. Když dojde v kybernetickém světě k nehodě, členové týmu musí vyšetřit, proč se nehoda stala a upozornit další týmy, jejichž kybernetická města mohou být ohrožena. Tím zabrání dalším nehodám po celém světě. Stejně tak jako policista nestojí na každém přechodu pro chodce, ani členové CSIRT týmů nejsou všude. Proto je potřeba myslet na to, že jsme to hlavně my sami, kdo je odpovědný za bezpečný pohyb v kyberprostoru.

Digitální stopa

Pokaždé, když něco napíšeme nebo dáme na Internet, je to jako bychom to nekonečně krát okopírovali a okopírované papíry rozdali lidem na letišti, kteří nastoupí do různých letadel a odletí na různá místa. My už se ale nikdy nedozvíme, kde naše dokumenty skončily, kdo k nim má přístup a zda je nějak neupravil. Když na každý papír napíšeme svou adresu, může nám zaklepat na dveře úplně cizí člověk a dožadovat se naší pozornosti, protože si bude myslet, že nás zná, když o nás obdržel takové informace. Pokud cokoliv píšeme nebo vkládáme na Internet, měli bychom vždy myslet na to, že už to nikdy nevygumujeme. Informace tam zůstanou navždycky a nepomůže ani ten nejsilnější prostředek, kterým tatínek uklízí ty nejzaschlejší stopy.

DNSSEC

Když chceme zavolat například mamince, často nevíme její telefonní číslo zpaměti. Stačí ale do seznamu v mobilu napsat „Maminka" a náš mobil už ví, jaké číslo maminka má. DNS funguje podobně. Díky němu můžeme do prohlížeče, skoro stejně jako do mobilu, namísto čísla 95.173.213.36 napsat maminka.cz. Počítač už si to sám na číselnou, správně řečeno IP adresu, přeloží a nám zobrazí požadovanou stránku. V době, kdy DNS vznikal, byl Internet bezpečným místem, jak ale narostl počet jeho uživatelů, snížilo se jeho bezpečí. DNSSEC představuje bezpečnostní rozšíření, které zajišťuje, že když se náš počítač ptá na to, co je na stránkách maminka.cz, nestane se, že by se nám zobrazily jiné, falešné nebo nakažené stránky, které jsou na jiné IP adrese.

Grooming

Člověk, který kontaktuje prostřednictvím Internetu vybranou osobu a po navázání důvěrného vztahu ji pozve na schůzku, ať už hrát počítačové hry nebo se podívat na štěňátka. Důvody k setkání volí různé. Na schůzce potom může oběť osahávat, fotografovat nebo přesvědčovat, aby začala podporovat teroristické a jiné extrémistické skupiny a hnutí, nebo zvolí jinou formu manipulace oběti. Vždy, než půjdete na schůzku s někým z Internetu, řekněte o tom svým rodičům, přátelům nebo někomu jinému, kdo vám bude moci zavolat a po schůzce si s nimi popovídejte o tom, jak schůzka probíhala a co se na ní dělo. Nikdy se s člověkem, kterého jste poznali přes sociální sítě, nescházejte na odlehlém místě nebo u něj doma.

Hacker

Hacker je často lupič, který však nevykrádá domovy a banky s pistolí, ale počítače a servery s nějakým programem. Způsoby, jakými to dělá, jsou různé. Stejně jako lupič může otevřít dveře pomocí falešného klíče, vlézt do bytu otevřeným oknem nebo si vymyslet nějakou příhodu, abyste ho do bytu sami pustili, může i hacker využít mnoha různých způsobů, jak se k vám do počítače vloupat. Slouží mu k tomu viry, trojské koně, phishingové stránky, vymyšlené příběhy, které vám zašle ve formě textové zprávy a další jednání, která spadají pod kybernetickou kriminalitu. Hacker však nemusí být vždy jen zlý, může působit i na straně dobra. Zlý hacker se odborně nazývá cracker.

Honeypot

V překladu se jedná doslova o hrneček s medem. Když nás obtěžují včely a vosy natolik, že si kvůli nim nemůžeme ani v klidu sníst zmrzlinu, je možné dát poblíž hrneček s medem a včely a vosy tak odlákat. Podobně je tomu u honeypotů v počítači. Útočníci stále vyvíjejí nové a nové varianty škodlivých kódů a hodní lidé se snaží naše počítače proti nim bránit. Ihned po odhalení nějakého nového škodlivého kódu vyvíjejí záplaty nebo nové verze aplikací. K detekci takových kódů slouží honeypoty, díky kterým je možné viry a jiné škodlivé kódy pozorovat.

IP adresa

IP adresy jsou něco jako telefonní čísla našich kamarádů. Každý má úplně jiné a my si je neumíme všechny pamatovat. Tato čísla však obsahují mnoho informací, například z jaké země kamarád je nebo jakého operátora používá. Lidská paměť si však všechna tato čísla neumí zapamatovat a ve své podstatě je pro nás důležité hlavně to, kdo nám volá a komu chceme volat. Neučíme se tedy čísla zpaměti, ale ukládáme si své kamarády pod jmény a přezdívkami do telefonních seznamů. Tato jména jsou stejná jako například jména webových stránek. Aby počítače poznaly, kde data a informace z webové stránky hledat, musejí stejně jako u telefonního čísla znát zemi, operátora, kterého představuje poskytovatel internetového připojení a místo, kde jsou data uložena.

Kybernetická kriminalita

I pomocí počítače lze často někomu velmi ublížit a je dokonce i časté, že kvůli nepříjemným zprávám, fotografiím a vydírání jsou lidé velice smutní. Díky počítačům lze také krást peníze z účtů jiných uživatelů. Každé jednání na Internetu, které nějak poškozuje druhé, může být označeno jako kybernetická kriminalita. Jako kybernetická kriminalita se dá označit mnoho jednání, se kterými se v pexesu seznámíte. Ransomware, viry, trojské koně, sexting, kyberšikana nebo zombie počítače. Je velice důležité proti nim bojovat například tak, že když na ně narazíme, nahlásíme je na webových stránkách www.stoponline.cz.

CZ.NIC | SPRÁVCE DOMÉNY CZ
BEZPEČNĚ NA NETU
Spolufinancováno Evropskou unií
Nástroj pro propojení Evropy

Kyberšikana

Když nám někdo poláme pastelky nebo roztrhne tričko, rodiče hned poznají, že nám někdo ubližuje. Můžou to s námi probrat a společně najít řešení. Když nám někdo ubližuje na Internetu, rodiče to často nemají jak zjistit. Obtěžující zprávy na mobil nám můžou chodit klidně i v noci a zlí spolužáci nebo neznámí lidé nám mohou prostřednictvím Internetu ubližovat třeba tím, že nám posílají ošklivé obrázky, nutí nás, abychom něco dělali nebo se nám jen kvůli něčemu posmívají. Pokud si s tím sami nevíme rady a nechceme se poradit s rodiči či paní učitelkou, můžeme se úplně tajně, klidně s použitím anonymního okna ve školním počítači zeptat např. na chatu linky bezpečí (www.linkabezpeci.cz) , která se pomocí v takovýchto situacích zabývá. Můžeme jim i zdarma zavolat na číslo 116 111.

Nomofobie

Někteří lidé jsou závislí na připojení prostřednictvím mobilních telefonů. Takoví lidé trpí nomofobií. Lidé závislí na mobilech a dalších zařízeních jsou vlastně skoro pořád k zastižení, když jim napíšeme, ihned odpoví, když jim zavoláme, povídají si s námi jak dlouho chceme, pořád dávají na net nějaké obrázky. Je super, že jsou pořád online, ale tito lidé už tady nejsou pro své blízké v opravdovém světě. Lidé trpící touto závislostí se často nepodívají na ta nejkrásnější místa naší planety, protože se bojí, že by nemohli být připojení k Internetu.

Phishing

Phishing pochází z anglického slova fishing (rybaření). Útočník je rybář a uživatelé Internetu jsou rybky. Když náhodou zatoužíme po nějaké potravě, se kterou ještě nemáme žádné zkušenosti, tak bychom vždy měli pečlivě prozkoumat, jestli v ní není náhodou nějaký skrytý háček. Když si nevíme rady, měli bychom se zeptat někoho zkušenějšího. Je potřeba vždy stahovat přílohy jen od lidí a ze stránek, které skutečně známe a kterým důvěřujeme. Také nikdy nesmíme zadávat svá hesla na stránky, které na nás náhodou někde vyskočí. Vždy, když na Internetu zadáváme heslo, měli bychom zkontrolovat, zda adresa stránky v prohlížeči odpovídá například názvu hračkářství, kde chceme na maminčinu platební kartu nakupovat dárky pro kamarády.

Pirátství

Většina z nás si myslí, že stahovat si filmy a hry na černo je v pořádku. Jenomže ono není. Představme si, že nakreslíme obrázek a pan učitel nám řekne, že tento obrázek můžeme příští týden na výstavě nabízet za tisíc korun. Jsme autorem, oprávněným prodat své dílo. Mezitím přijde spolužák, obrázek si tajně okopíruje nebo obkreslí a začne jej nabízet za 500 korun. Když potom přijdeme na výstavu, o náš obrázek už nikdo nemá zájem, protože už ho všichni mají. To přeci není v pořádku. Pokud by se to nelíbilo nám, těžko se to bude líbit někomu jinému. Řešením je nestahovat filmy a hry, které nahrávají jiní lidé na Internet bez toho, aby k tomu měli svolení autora, tedy naše svolení, že mohou obrázek okopírovat a nabídnout dalším lidem.

Ransomware

Když zadáváme PIN do mobilu a třikrát se spleteme, zablokuje se nám SIM karta a my musíme zadat dlouhé složité číslo (PUK), abychom SIM kartu odblokovali. Ransomware je o to horší, že nám může zablokovat přístup k úplně všem našim složkám v mobilu, tabletu nebo počítači. Můžeme tak přijít o všechny své zprávy, fotky a další věci. Vždy, když nám na Internetu přijde nějaká žádost o peníze nebo výhrůžka, abychom něco udělali, jinak že nás postihne něco špatného, ihned bychom to měli říct rodičům, vyfotit společně s nimi obrazovku, na které výhrůžka je a nahlásit to na policii nebo na www.stoponline.cz. Hlavně se vy ani rodiče nikdy nesnažte nic zaplatit. Vždy je lepší přiznat se, že jsme navštívili zakázané stránky, než podporovat zločince.

Router

Krabička, díky které se můžeme připojovat k Internetu z mobilu, z tabletu i počítače. Když router necháme dlouho bez povšimnutí a osamocený, může klidně onemocnět, protože je stejně zranitelný jako naše počítače, kterým jak už víme, je nutné pomáhat se záplatováním. Bohužel na zdraví těchto krabiček nezapomínáme jen my, ale i ti, kdo je vyrábějí. Často se tedy stává, že i když krabičky mají díry, záplaty na jejich díry nejsou nikde k sehnání. Takové krabičky potom mohou být úplně celé zavirované a od nich se mohou nakazit i naše mobily, tablety a počítače, o které se pečlivě staráme. Abychom tomu předešli, je nutné říct rodičům, aby kupovali jenom takové routery, u kterých je možné provádět jejich pravidelné aktualizace. Jedním z takových je Turris Omnia.

Řetězový dopis

Určitě to znáte. Čtete si nějakou zajímavou zprávu a najednou je tam napsáno: „Pošli tuto zprávu dalším lidem nebo nebudeš mít štěstí." Když na takové zprávy reagujeme, chodí nám potom častěji a častěji. Navíc se stává, že se takto šíří na Internetu úplně falešné zprávy, třeba o tom, že nemocné dítě potřebuje pomoci nebo že štěňátka budou utracena. Pokud nás dané zprávy zaujmou, měli bychom si nejdříve ověřit, jestli tato štěňátka nebo děti opravdu existují nebo zda se jedná o hoax, tedy úplně nebo částečně vymyšlený příběh, kterých je Internet plný. Pokud informace nikde jinde nemůžeme najít, je dobré takovou zprávu už dál neposílat.

Sdílení

Často chceme sdílet příběhy, které v životě prožíváme. To samo o sobě vůbec nevadí, ale když na Internetu cokoli sdílíme, musíme být připraveni na to, že se nás na to budou lidé třeba ptát. Někteří se nám pak mohou za naše příspěvky i smát. Pokud nechceme, aby k takovým situacím docházelo, můžeme se o tyto informace dělit jen s lidmi, kterým skutečně důvěřujeme. Je proto dobré si nastavit příspěvky jako soukromé a tedy viditelné jen pro toho, koho si sami vybereme. Fotografie a další soubory je možné zase dát do složky, kterou zabezpečíme heslem a to dáme jen našim kamarádům.

Sexting

Příklad toho, jak moc nám může digitální stopa ublížit. Někteří lidé zasílají svým kamarádům, svému klukovi nebo holce fotky, na kterých jsou ve spodním prádle nebo i bez něj. Tyto fotky se nedají už nijak vzít zpět a často je vidí i celá třída. Spousta těch, kdo odesílají takové fotografie, si vůbec nepřipouští, že by je mohli vidět i další lidé. Ve chvíli kdy se to stane, tak se tolik stydí, že to ani neřeknou nikomu, kdo by jim pomohl. Pokud byste někdy takovou chybu udělali a na základě ní byli šikanováni a ponižováni, jedná se o kyberšikanu. Navíc je zveřejňování našich fotografií bez našeho souhlasu protizákonné, takže existuje obrana. Nejlepší ale samozřejmě je, dávat na Internet jenom to, s čím byste se klidně osobně pochlubili před celou třídou.

Soukromí

I když se často zdá, že do našeho počítače nemůže nikdo vidět, není to pravda. Naše e-maily, fotografie a další data jsou uložená na různých serverech, kam se mohou dostat různí lidé. Udržet soukromí v počítačích připojených k Internetu je velmi komplikované. Čím více překážek však hackerům postavíme do cesty, tím náročnější bude se k našemu soukromí dostat. Je důležité neukládat žádné soukromé věci na neznámá úložiště na Internetu, aktualizovat naše zařízení včetně routerů a používat silná hesla. Nezbytně nutné je také dávat pozor na to, co sami o sobě na Internetu prozrazujeme, protože vždy, když máme veřejný profil, může kdokoli na světě zjistit kde jsme, co děláme nebo jak se cítíme a pokusit se toho nějak využít.

SPAM

Hromada nepotřebných informací, které nám chodí prostřednictvím Internetu nebo SMS zpráv a o které vůbec nestojíme. Kvůli spamu můžeme úplně ztratit orientaci ve své poště a snadno přehlédnout nějakou důležitou zprávu. K tomu, aby se k nám záplava nevyžádaných informací nezačala odevšad nekontrolovatelně hrnout, je potřeba dávat pozor pokaždé, když souhlasíme s obchod-

CZ.NIC | SPRÁVCE DOMÉNY CZ
BEZPEČNĚ NA NETU
Spolufinancováno Evropskou unií
Nástroj pro propojení Evropy

ními podmínkami anebo udělujeme jiný souhlas na Internetu. Vždy je důležité otevřít si podmínky, se kterými se chystáme souhlasit, nalistovat kapitolu s názvem Ochrana osobních údajů a zkontrolovat, jestli se tam píše, že naše údaje nebudou poskytovány třetím osobám, to znamená dalším lidem, kteří by je mohli použít dále.

Šifrování

Slovem šifra nebo šifrování označujeme postup, který převádí čitelnou zprávu na její nečitelnou podobu. Zašifrovaný text lze rozluštit jenom v případě, že známe správný klíč. Šifrovat můžeme data na pevném disku, přenosném médiu, jakým je například USB disk nebo flash karta, ale i celou naši komunikaci jako jsou zprávy a e-maily. Dalším způsobem šifrování jsou virtuální privátní sítě (VPN), které si můžeme představit jako takový tunel, o kterém vědí pouze ti, kdo ho používají. Dalším místem, kde se uplatňuje šifrování, jsou webové stránky. Stránku s šifrovaným přenosem dat poznáme tak, že webová adresa začíná písmeny https místo http a zobrazuje se u ní ikonka zamčeného zámečku.

TLS/SSL certifikát

Tyto zkratky souvisí s šifrováním, konkrétně s šifrováním webových stránek. Stránku s šifrovaným přenosem dat poznáte podle toho, že začíná písmeny https místo http. Kromě toho, že protokol https zajišťuje šifrování toho, co na Internet píšete, umožňuje také ověření, zda stránky, na kterých zrovna jsme, jsou opravdu těmi, na které jsme chtěli jít. Díky TLS/SSL certifikátům lze předejít útokům různých rybářů, kteří nás zkoušejí nachytat na své háčky - phishingové stránky. Https se také používá všude tam, kde si prohlížeč a server vyměňují nějaké citlivé informace, například přihlašovací jméno a heslo.

Trojský kůň

Trojský kůň byl ve starých řeckých bájích a pověstech obrovský dřevěný kůň, do kterého se ukryli vojáci, kteří chtěli napadnout město Tróju. Podobnou lest využívají zlí lidé na Internetu. Snaží se nás přesvědčit, že nám nabízí něco užitečného, zajímavého nebo výhodného a když si to za hradby svého počítače přivezeme, tedy, když si to stáhneme z Internetu, vyskáčou nám do počítače lstivé programy, které otevřou brány dalším a dalším zlomyslným útočníkům. K tomu, abychom si za hradby svého počítače nepřivezli Trojského koně, stejně hloupě jako obyvatelé Tróji, je potřeba vždy vše stahovat pouze z oficiálních stránek či tržišť a nedopouštět se internetového pirátství.

Uživatelské jméno/heslo

Stejně jako klíče od bytu, slouží uživatelské jméno a heslo, kterým se dohromady říká přihlašovací údaje. Na svých účtech máme spoustu cenných informací a můžeme být díky nim v kontaktu se svými kamarády. K tomu, aby naše účty nikdo nevykradl, je potřeba se o ně zodpovědně starat. U hesla je navíc dobré, aby obsahovalo vždy nějaká písmenka, čísla a speciální znak, třeba hvězdičku. Také je důležité heslo nepsat na papírky a mít více hesel k různým účtům. Třeba k účtu, kde máme jen fotky se třídou, není potřeba mít dlouhé a složité heslo, protože to nejsou žádné tajné fotky a pravděpodobně i kdyby je někdo smazal, tak nám je spolužáci pošlou znovu. Vždy je potřeba pečlivě zvažovat, co na účtech uchováváme.

Útok

Stejně jako chodíme pravidelně na kontrolu, aby se nám nekazily zoubky a nemusel nám je pan zubař složitě napravovat, měli bychom kontrolovat i počítače, mobily a tablety. Pokud pravidelně neinstalujeme aktualizace, nepoužíváme antivir a stahujeme hry a aplikace z neoficiálních stránek, mohou náš počítač napadnout zlí hackeři a zneužít jej k rozesílání spamu, vyřazení nějakého systému z provozu, k napadení stránek naší školy k tomu, aby ukradli peníze z bankovních účtů nebo k dalším zlým věcem. Je opravdu důležité kontrolovat, v jakém stavu máme svá zařízení, aktualizovat aplikace, nestahovat neověřené programy a pravidelně aktualizovat i antivirový program.

Virus

Když jsme nemocní, tak jsme často rádi, že můžeme ležet v posteli, těžko se nám obléká, chodí nebo i pije. Počítače jsou na tom úplně stejně. Když chytnou nějaký vir, jejich funkce se mohou změnit. Mohou být pomalejší nebo začít dělat něco, co jsme jim nezadali, aby dělaly. Zavirovaný počítač dokáže nakazit další počítače a díky tomu může hacker potom útočit na nějaké velké organizace jako je třeba škola, obchod nebo stránky, kde je napsáno, jak jezdí vlaky. Viry také můžou posílat útočníkům naše přihlašovací údaje nebo i všechno, co na počítači děláme, včetně našich tajných zpráv. Pro předcházení nakažení je důležité mít nainstalovaný antivir i v tabletu a mobilu.

Wi-Fi

V obchodních centrech, restauracích a kavárnách, ale i v autobusu či ve vlaku se dnes můžeme připojit k bezdrátové síti neboli Wi-Fi. Veřejné Wi-Fi sítě musí být co nejsnadněji použitelné, protože jsou určeny velkému množství lidí a zařízení. Je tedy docela logické, že nejsou úplně nejlépe zabezpečené. Na veřejné Wi-Fi síti si šikovnější hacker může klidně přečíst, co na Internetu děláme, kam se přihlašujeme a také odposlechnout naše přihlašovací údaje a hesla. Buďme tedy při využívání veřejných Wi-Fi sítí vždy velice opatrní při rozhodování o tom, kam se prostřednictvím ní přihlásíme a jaké údaje z veřejné Wi-Fi do Internetu pošleme.

Zálohování

Zálohování znamená uložení informací z našich zařízení do bezpečí nějakého externího zařízení pro případ, že by se nám někdy stalo, že nám začne někdo vyhrožovat smazáním všech dat tak, jak jsme si to popsali u Ransomwaru. Vedle napadení virem se náš počítač může i rozbít. Pro zálohy věcí, které nejsou citlivé, je nejlepší používat on-line zálohování, např. Crashplan, Mozy, Dropbox, Carbonite a další, které průběžně nahrávají vše, co máme ve vybrané složce, a navíc se k daným souborům můžeme dostat odkudkoliv. Soubory, kde máme něco tajného, bychom však měli uchovávat pouze na externích discích.

Záplata

Když se roztrhne pytel, začne se z něj ven sypat mouka. Stejně tak to mají počítače. Pokud se jim něco „roztrhne“, mohou se z nich začít ven sypat data, tedy naše hesla, fotky, zprávy, které si vyměňujeme s kamarády a další důležité věci. Ve chvíli, kdy k tomu dojde, je nutné počítač co nejdříve záplatovat. To znamená, že se vyvine kousek programu, který pasuje na místo, které je děravé a tam se nainstaluje. Takovému procesu se říká aktualizace. Záplata se dává dovnitř do počítače na jednotlivé programy včetně operačního systému. K tomu, aby se záplata mohla co nejdříve dostat na správné místo, potřebujeme pravidelně spouštět instalaci aktualizací.

Zombie

Zombie počítač se od toho klasického liší tím, že jej podobně jako Zombíka v nějakém strašidelném filmu ovládá zlá moc. Hacker se zlými úmysly nám nějakým způsobem, ať už pomocí viru, trojského koně nebo jinak nahraje do počítače program, prostřednictvím kterého je možné náš počítač úplně ovládnout. To znamená, že útočník z našeho počítače může klidně posílat spam, šířit pomocí něj trojské koně, vydělávat si peníze za reklamu nebo se přihlašovat na nějaké stránky, pomocí čehož úplně zahltí server.

CZ.NIC | SPRÁVCE DOMÉNY CZ
BEZPEČNĚ NA NETU
Spolufinancováno Evropskou unií
Nástroj pro propojení Evropy