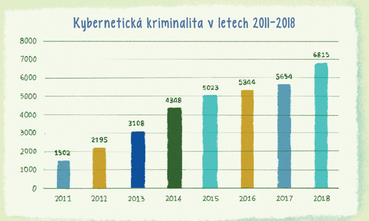
Kyberkriminalita

Jedná se o takovou trestnou činnost, pro kterou jsou jako nástroj používány moderní informační a komunikační technologie, tedy počítače, mobilní telefony a internet. Počet trestných činů v této oblasti každoročně stoupá a obětí se může stát každý z nás.



Doporučení:

- V prostředí internetu nikdy nesdělujme citlivé a osobní informace neznámým lidem.
- Nikomu neposílejme přihlašovací údaje ke svým účtům (e-mail, bankovnictví, sociální sítě).
- Důvěřujme, ale prověřujme – především při nákupech z e-shopů i od soukromých prodejců.
- Pamatujme, že i na internetu se pohybují lidé jako my – nenechme se pod domnělou rouškou anonymity zlákat k neslušnému až urážejícímu chování vůči druhým.

Kyberšikana

Kyberšikana je šikana přes internet a mobilní telefony, kdy je obět opakovaně a dlouhodobě záměrně ponižována jedním, ale častěji více agresory. Oproti šikaně tváří v tvář má kyberšikana jednu zásadní nevýhodu – nikdy nekončí. Mezi oběťmi i pachateli nalezneme jak děti, tak i dospělou populaci.

Doporučení:

- Zbystřeme, pokud naše dítě odchází od počítače smutné, plačtivé, nebo naopak přemíru veselé.
- Nepokračujme v komunikaci s útočníkem.
- Nikdy nic nemažme – SMS, e-maily i konverzace ze sociálních sítí mohou sloužit jako důkazy pro případné vyšetřování Policií ČR.
- Nezůstávejme s kyberšikanou sami – obraťme se s žádostí o pomoc na svou rodinu, přátele, školu, psychologa, či přímo na Policii ČR.

Nezákonný on-line obsah

V prostředí internetu se můžeme (ne)vědomky dopouštět trestných činů pouným zveřejňováním, přeposíláním či stahováním obsahu, ke kterému nemáme autorská práva, ale také šířením pomluvy, útoky proti druhým lidem či nenávistnými komentáři.

Doporučení:

- Hudba, filmy, fotografie, knihy, vědecké práce a další díla jsou chráněna autorským právem. Bez svolení autora je nemůžete z internetu stahovat, kopírovat, distribuovat nebo vydávat za své.
- Zvažme, zda je pro vás používání tzv. P2P sítí výhodné – i zde se můžeme dopouštět trestného činu, pokud s ostatními sdílíme nelegální obsah.
- Pomluva, schvalování trestného činu, hanobení národa a rasy, nebo podněcování nenávisti ke skupině osob jsou trestné činy. Mysleme na to vždy, když budeme chtít napsat nějaký peprný příspěvek do internetových diskuzí. Naše svoboda slova není neomezená a anonymita na internetu pouze domnělá.

Neoprávněný přístup k počítači/hacking

Do našeho počítače se nám útočníci mohou dostat několika způsoby. Zneužitím naší důvěry, krádeží či odkoukáním hesel při jejich zadávání, ale také přes speciální programy, které si stáhneme k sobě do počítače třeba jako přílohu e-mailu.

Doporučení:

- Nesdělujme nikomu přístupové údaje k žádnému z našich účtů, ani je neposílejme e-mailem či SMS zprávou.
- Své přihlašovací údaje s hesly si nikam nepíšme.
- Soukromé domácí WiFi sítě mějme zaheslované, nikoli veřejné.
- Nestahujme si e-mailové přílohy od neznámých lidí, ani neklikejme na odkazy, které nám posílají.
- Používejme renomovaný antivirový program a pravidelně ho aktualizujme, a to i v mobilu.

Podvodné e-shopy a nákupy na internetu

Podle dat Asociace pro elektronickou komerci utratili Češi v roce 2018 na internetu 135 miliard korun. Vzrůstající obliby pohodlných nákupů z tepla domova si jsou ale vědomi i podvodníci. Věnujme proto při svých nákupech přes internet čas výběru nejen kvalitního zboží, ale také kvalitního prodejce.

Doporučení:

- Zjistěme si co nejvíce informací o e-shopu nebo soukromém prodejci.
- U neověřeného e-shopu/prodejce doporučujeme platit dobírkou.
- Při objednávání zboží ze zahraničí si spočtěme, na kolik nás vyjde poštovné, DPH a clo.
- Zajímejme se o to, jak budeme moci postupovat při reklamacích či vracení zboží do zahraničí.
- Doprava zdarma ze zahraničních, často čínských, e-shopů bývá vykoupena dlouhou dodací lhůtou v řádu týdnů až měsíců.

Ransomware

Ransomware je vyděračský software, který má za úkol znepřístupnit majiteli jeho počítačové soubory, nebo rovnou celý systém. Za obnovení funkčnosti vyžaduje vydírač zaplacení výkupného, nejčastěji ve virtuální měně Bitcoin nebo v jiné tzv. kryptoměně.

Doporučení:

- Nestahujme si přílohy a soubory od neznámých lidí, nenavštěvujme pochybné internetové stránky a pravidelně aktualizujme antivirový program.
- Dbejme i na zabezpečení domácí wifi sítě, vždy ji mějme zaheslovanou.
- Nevstupujme do komunikace s útočníkem a nikdy mu nic neplaťme.
- Pokusme se odstranit ransomware klasickým antivirovým programem, případně oslovme IT specialistu.
- Pokud je infikovaný firemní počítač, bezodkladně to oznamme svému nadřízenému.

KRAJE PRO BEZPEČNÝ INTERNET

WWW.KPBI.CZ

KRAJE ZAPOJENÉ DO PROJEKTU

PARTNEŘI PROJEKTU

Šíření pornografie/sexting

Šíření (dětské) pornografie, výroba a jiného nakládání s dětskou pornografií či zneužití dítěte k výrobě pornografie jsou trestné činy. O sextingu mluvíme v případě zasílání soukromého intimního materiálu mezi životními partnery. I tento materiál však může naplňovat skutkovou podstatu trestného činu.

Doporučení:

- Nestyďme se s dětmi mluvit o nahotě – vysvětleme jim, že nahota je soukromá věc, která by se neměla nikde vystavovat.
- Nezveřejňujme soukromé nahé nebo odhalené fotky ať už své, nebo svých dětí.
- Budujme se svými dětmi důvěru – jen ta nám pomůže ve chvíli, kdy se dítě dostane třeba do situace, kdy ho bude někdo vydírat kvůli nahým fotkám.
- V případě zneužití jakéhokoli materiálu se sexuálním podtextem kontaktujme Policii ČR.

Fake news

Fake news jsou smyšlenými, úmyslně zmanipulovanými zprávami z oblasti politiky, životního prostředí a dalších společenských problémů, které se tváří jako seriózní zpravodajství. Základem může být skutečná událost, která je ale účelově upravena a překroucena s cílem ovlivnit veřejné mínění.

Doporučení:

- Pro fake news je typická přemíra otazníků a vykřičníků v textu, i absence autora textu.
- Fake news se snaží v příjemci zprávy vyvolat silné emoce, a to především ty záporné, jakými jsou strach, zloba nebo nenávist.
- Důvěřujme, ale prověřujme. Pátrejme po zdrojích a jejich důvěryhodnosti. Pokud známá a renomovaná média tuto zprávu nezveřejnily, pak nejspíše proto, že je nepravdivá.
- Varování a fámy všeho druhu nazýváme hoax, který se mezi lidmi šíří řetězově.

CEO podvody

CEO podvod je zaměřený především na velké firmy či státní instituce. Podvodníci se z firmy snaží vylákat nemalé finanční částky pod záminkou tajné fúze nebo choulostivé situace, ale také zkouší posílat faktury na neexistující zboží a služby. Zneužívají jména generálního či finančního ředitele.

Doporučení:

- V případě, že nás kontaktuje vysoký manažer firmy, se kterým nejsme běžně ve styku, ověřme si, že jsme komunikovali opravdu s ním. Třeba mu zavolejme na jiné telefonní číslo, než ze kterého nám on sám volal.
- Nenechme se zahnat do časové tísně. Když na nás někdo naléhá, lichotí nám, žádá nás o nestandardní úkon v rozporu s interními postupy, nebo si přeje zachovat absolutní důvěrnost, je to pro nás znamení, že je něco špatně. Dopřejme si čas na prověření celé situace.
- Vyhněme se sdílení informací o organizační struktuře naší společnosti, bezpečnosti nebo pracovních postupech, a to jak na webových stránkách firmy, tak i na sociálních sítích.

Internet věcí

Internet věcí (Internet of Things, IoT), označuje chytrá zařízení, stroje či celé objekty, které jsou schopné díky internetu mezi sebou komunikovat, a to bez ohledu na vzdálenost. Během roku 2019 bude do IoT zapojeno celosvětově 8,3 miliardy zařízení, a to především v domácnostech.

Doporučení:

- Zvažme, zda naše pohodlí stojí za ztrátu soukromí.
- Zajímejme se, kam se data z našich přístrojů posílají, ukládají a dále zpracovávají. Pokud s výsledným zjištěním nebudeme spokojeni, nemusíme v používání té které technologie dále pokračovat.
- Pravidelně aktualizujme všechna naše zařízení připojená na internet, domácí WiFi mějme zaheslovanou.
- IoT také zachraňuje životy – ať už v autech přes systém eCall, nebo třeba v cyklistických helmách, které po silném nárazu samy zavolají o pomoc.

POZOR NA KYBERPROSTOR!