

1. HESLA



Které z níže uvedených hesel je nejslabší?

- a) Ani4ka05
- b) QWERTY
- c) Radek2007@
- d) R\$obot\$201
- e) Chytrej\$borec@
- f) MySak999#



Čas, který trvá použití AI k prolomení vašeho hesla^[2023]

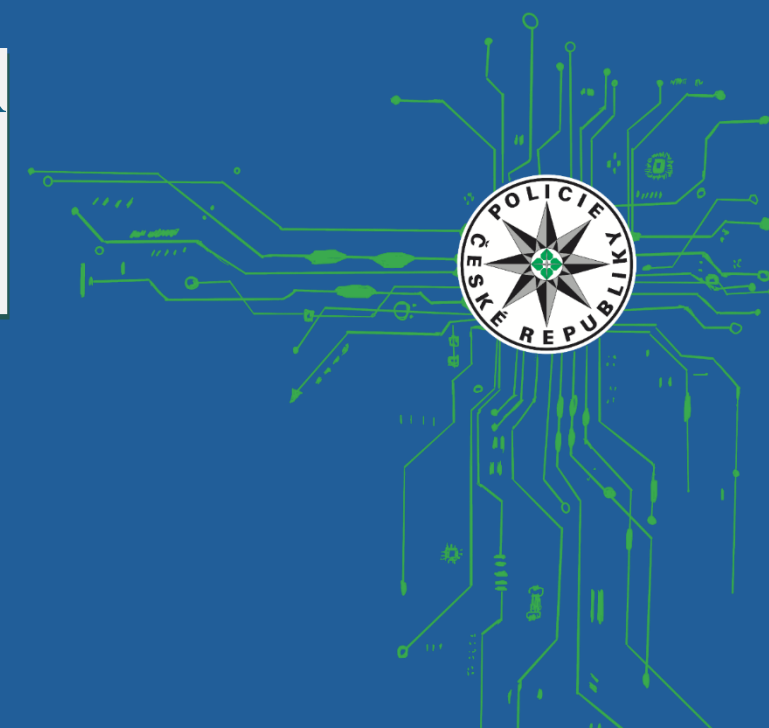
# CHARAKTERU	Pouze čísla	Malá písmena	Velká a malá písmena	Číslo, velká a malá písmena	Číslo, velká a malá písmena, symboly
4	Okamžitě	Okamžitě	Okamžitě	Okamžitě	Okamžitě
5	Okamžitě	Okamžitě	Okamžitě	Okamžitě	Okamžitě
6	Okamžitě	Okamžitě	Okamžitě	Okamžitě	4 sekundy
7	Okamžitě	Okamžitě	22 sekund	42 sekund	6 minut
8	Okamžitě	3 sekundy	19 minut	48 minut	7 hodin
9	Okamžitě	1 minut	11 hodin	2 dny	2 týdny
10	Okamžitě	1 hodina	4 týdny	6 měsíců	5 let
11	Okamžitě	23 hodin	4 roky	38 let	356 let
12	25 sekund	3 týdny	289 let	2000 let	30 tisíc let
13	3 minuty	11 měsíců	16 tisíc let	91 tisíc let	2 miliony let
14	36 minut	49 let	827 tisíc let	9 milionů let	187 milionů let
15	5 hodin	890 let	47 milionů let	613 milionů let	14 miliard let
16	2 dny	23 tisíc let	2 miliardy let	26 miliard let	1 Tr let
17	3 týdny	812 tisíc let	539,72 milionů let	2 Tr let	95 t let
18	10 měsíců	22 milionů let	7,23 miliard let	96 Tr let	

- **Nastavte si silné a unikátní heslo** pro každý účet. Pokud se někomu podaří odhalit vaše univerzální heslo, získá přístup k veškerým vašim datům. Silné heslo obsahuje alespoň 16 znaků, malá a velká písmena, číslice a speciální znaky.
- **Aktivujte si dvoufázové ověření**, můžete si nastavit ověření přes SMS, aplikaci v mobilním telefonu nebo přes e-mail.
- **Svá hesla si chraňte**, nikomu je nesdělujte a nezadávejte je v přítomnosti ostatních. Nikdy je nezapisujte do nechráněného dokumentu nebo diáře. K ukládání hesel můžete používat **bezpečnostní aplikace** typu „správce hesel“.



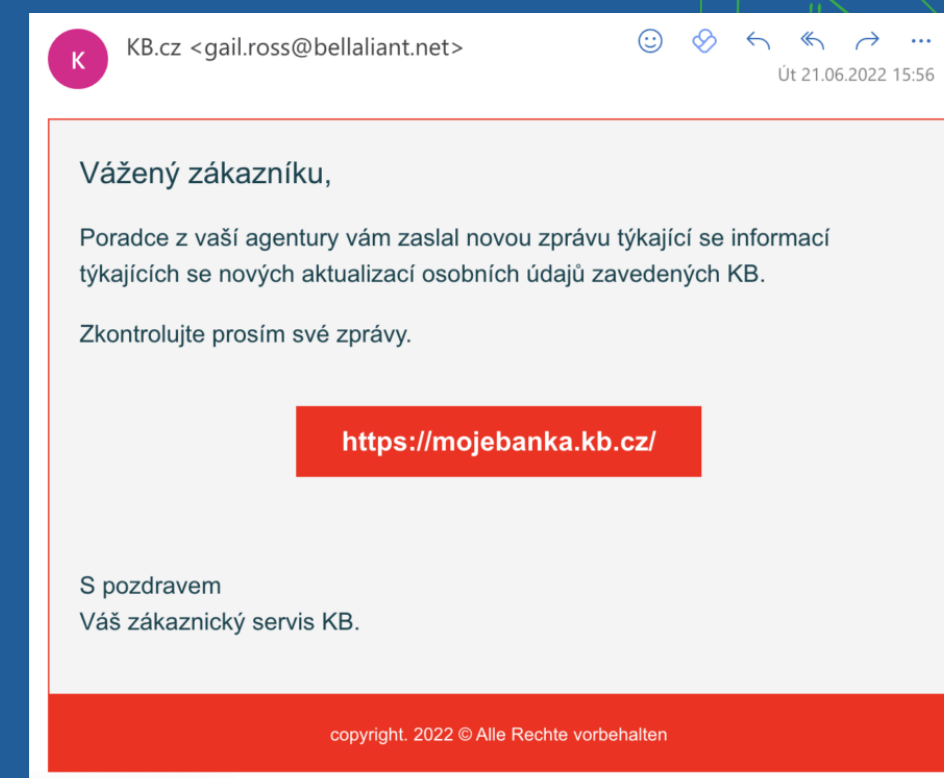
2. PHISHING (*čti fišing*)

KYBERSTEZKA S PČR



Jak rozeznat phishingový útok přes e-mail?

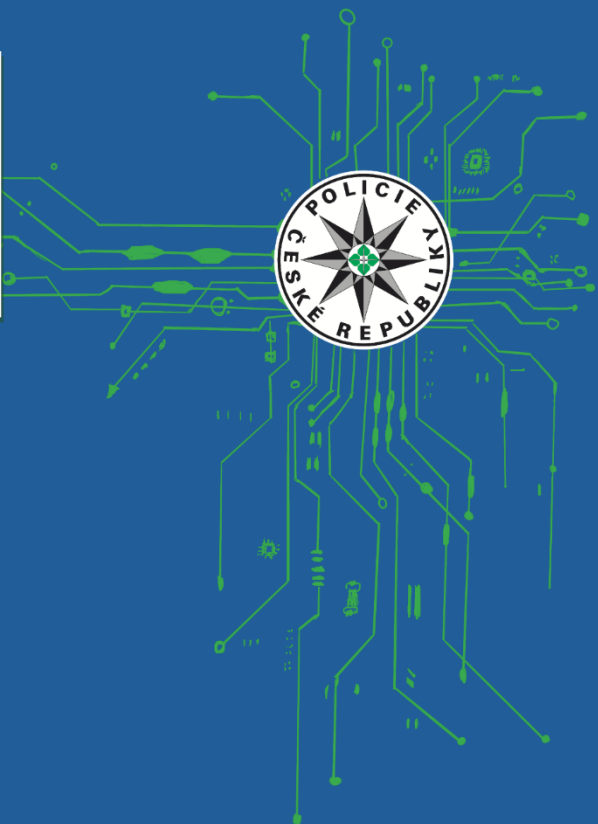
- a) podle hlavičky emailu, ověření https:// stránek, jazykových nesrovnalostí, přesměrování na podezřelé webové stránky
- b) podle barevného provedení stránek a e-mailu
- c) nemusím nic ověřovat, mě se nikdy nic nemůže stát
- d) ověřím tím, že na e-mail odepíšu
- e) kliknu na odkaz v e-mailu, vyplním údaje o své osobě, platební kartě a budu čekat, co se stane
- f) podle délky textu a obrázků



- **Adresu odesílatele si ověřujte** pomocí náhledu do hlavičky e-mailu. Zobrazí se vám najetím kurzoru na jméno odesílatele. Podvodníci se často vydávají za nadřízeného, kolegu či banku a posílají falešné faktury či příkazy. **Všímejte si také nejasností a jazykových nesrovnalostí** (lámaná čeština, absence diakritiky, špatný slovosled) - může jít o strojový překlad. Pokud se vám e-mail zdá podezřelý, ověřte jeho pravost osobně či telefonicky.
- **Neotvírejte přílohy z neznámých zdrojů**, mohou obsahovat škodlivý program (malware). **Neklikejte na odkazy v podezřelých e-mailech**, ty mohou vést na podvodné stránky, které se snaží vylákat vaše osobní údaje, zejména přihlašovací jméno a heslo, které pak zneužijí ke krádeži účtu (phishing).



3. PLATBY NA INTERNETU



K čemu slouží CVV kód na zadní straně karty?

- a) k potvrzení příjmu peněz na platební kartu
- b) k předání kupujícímu společně s číslem platební karty
- c) trojmístné číslo, kterým autorizuji (potvrzuji) platby na internetu. K platbě musím zadat číslo platební karty a následně kód CVV. Při platbě na internetu nahrazuje PIN.
- d) k zadání do formuláře, který mi přijde jako nevyžádaná pošta do e-mailu
- e) nevím, stejně jako nečtu, co potvrzuji ve svém bankovníctví za platby a na jaké částky
- f) pro komunikaci s bankou

Video k online nákupu



Zapamatujte si: K obdržení finančních prostředků slouží číslo účtu a kód banky. K platbě/úhradě zadáváme číslo platební karty a CVV (card verification value) kód.



4. SEXTING

KYBERSTEZKA S PČR



Je trestné přeposílat přes internet intimní (nahou) fotku 15ti leté dívky?

- a) Ne, sama fotku vytvořila, tak jí asi nevadí posílání fotografie dál
- b) Ne, je starší 15 let a tudíž trestně odpovědná, takže přeposlat fotku nevadí
- c) Ano, pokud by jí to vadilo
- d) Ano, do 18 let je dle zákona dítětem a při přeposílání bychom se dopustili „jiného nakládání s dětskou pornografií“
- e) Ne, ale musím mít její souhlas
- f) Ano, ale na internetu je vše anonymní, tak nikdo nezjistí, kdo fotku přeposlal



Video PČR: Say NO!

Video "fotka nikdy nezmizí"

Video k sextortion (vydírání)



Sexting může být rizikový, protože pokud někomu poskytneme svou vlastní fotografii, může ji zneužít proti nám – například ji použít k našemu vydírání, vyhrožování, může ji rozšířit po internetu apod. Pokud se intimní fotografie dostane na internet, je velmi obtížné – téměř nemožné – se jí zcela zbavit.

5. WHATSAPP SCAM



Přijde vám zpráva z neznámého čísla s následujícím textem, co uděláte?

„Ahoj mami, tohle je moje nové číslo. Můj telefon je rozbitý. Pošli mi zprávu na whatsapp na tel:.....“ V další konverzaci následuje prosba o rychlou finanční pomoc, jelikož se nemůže Váš potomek přihlásit, kvůli změně tel. čísla do svého bankovníctví a musí urychleně něco zaplatit.

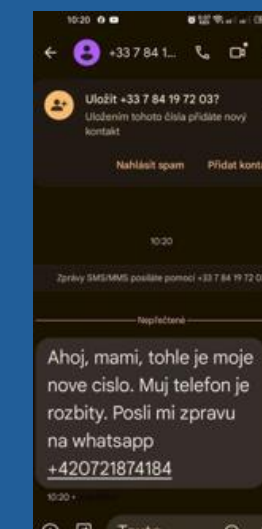
- Je to můj syn/dcera, takže mu/jí samozřejmě pomůžu a podle instrukcí odešlu peníze na účet, i když je zahraniční a jméno příjemce neznám.
- Zavolám dceři/synovi na původní tel. číslo a nebo ho/jí kontaktuji přes messenger, či whatsapp na předešlém kontaktu a zeptám se, zda mi posílal zprávu, že má rozbitý telefon.
- Chvilí váhám, prověřím si telefonní číslo, které mi syn/dcera poslal, že je jeho nové a když nenajdu nic podezřelého, tak v komunikaci s mým potomkem pokračuji a peníze v klidu pošlu.
- Zavolám dceři/synovi na původní tel. číslo a když mi to nezvedá, usoudím, že má opravdu telefon rozbitý a dbám instrukcí a peníze pošlu.
- Jelikož nemám tolik finančních prostředků, kolik potřebuje můj syn/dcera uhradit, tak si vezmu rychlou půjčku přes mé bankovníctví a peníze rychle pošlu, aby se nedostal/la do problémů.
- Nejdřív si zprávy nevšímám, ale když mi přijde po druhé, tak zpozorním. Nevadí, že moje dítě neví, jak se jmenuji, ani kdy jsme se naposledy viděli, zjevně potřebuje rychle pomoci a i když je teprve na základní škole, tak fakturu zaplatím.

Píše vám někdo z Vašich blízkých a žádá o pomoc? Spojte se s ním telefonicky! Ptejte se na věci, které může znát jen skutečný příbuzný!
**ŠMEJDI DOKÁŽÍ
NAPODOBIT
JAKÉKOLI ČÍSLO!**

Jak se bránit Zavolejte zpět na původní číslo nebo využijte jiný komunikační kanál (Facebook, Skype, Teams). Položte otázku, na kterou znáte odpověď jen vy dva – například jméno rodinného mazlíčka z dětství.

Dávejte si pozor na naléhavé prosby. Jakýkoli tlak na rychlé jednání je podezřelý. Nikdy neposílejte peníze ani osobní údaje, dokud si nejste jistí, kdo je na druhé straně. Podezřelý účet na WhatsAppu zablokujte a nahlaste – aplikace ho následně prověří. O podvodech mluvte i se svými rodiči či prarodiči – prevence je nejúčinnější obranou.

Video o podvodných taktikách



6. UMĚLÁ INTELIGENCE (AI)

KYBERSTEZKA S PČR



Jak lze zneužít umělou inteligenci k páčání trestné činnosti?

- a) Nelze jí zneužít
- b) Lze zneužít k podvodům se syntetickou identitou, technologie deepfake
- c) Nelze zneužít, jelikož umělá inteligence slouží i k detekci anomálií v dokumentech a komunikačních vzorcích
- d) Nelze, jelikož užitím AI k trestné činnosti by znamenalo postih
- e) Nikdo by užití umělé inteligence neodhalil, takže si jí můžu využívat, jak chci
- f) Lze, ale umělá inteligence podvod sama zastaví a oznámí Policii

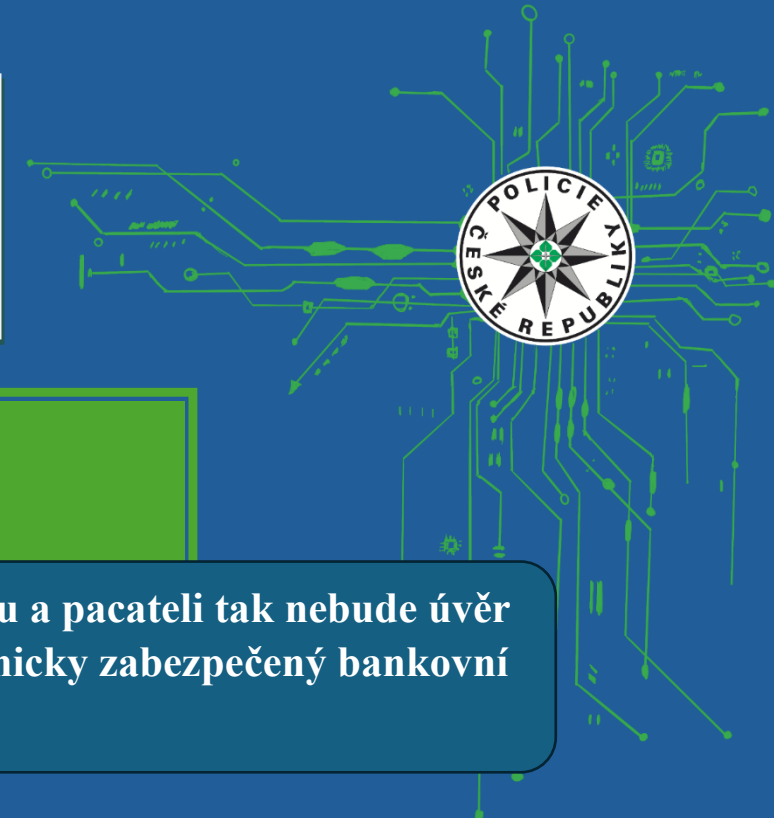
Video k umělé inteligenci



- **Umělá inteligence**=Počítačová věda, která se zabývá schopností strojů/programů napodobovat lidské schopnosti (učení, řešení problémů, kreativita, plánování)
- **Deepfake**=technologie, která umožňuje vytváření falešného digitálního obsahu pomocí algoritmů strojového učení, které dokáží realisticky nahradit tváře a hlasové stopáže v existujících, fotografiích anebo zvukových nahrávkách. Upravuje se především mimika obličeje a řeč jednotlivých aktérů.
- Strojové učení= zaměřuje se na to, jak naučit stroje učit se z dat a zlepšovat se zkušenostmi (trénovat)
- Zveřejňováním videí a fotografií na internetu se sami vystavujeme hrozbě zneužití materiálu nejen přes umělou inteligenci.



7. SPOOFING



Zavolá vám policista s následující zprávou, co uděláte?

Přesvědčuje vás o tom, že si na vás chce vzít někdo úvěr a bude po Vás chtít, abyste si vzali půjčku, čímž překročíte svoji bonitu a pacateli tak nebude úvěr poskytnut, přičemž musíte jednat rychleji, než pachatel. Následně máte veškeré peníze vybrat v hotovosti, nebo poslat na technicky zabezpečený bankovní účet dle pokynů pracovníků ČNB.

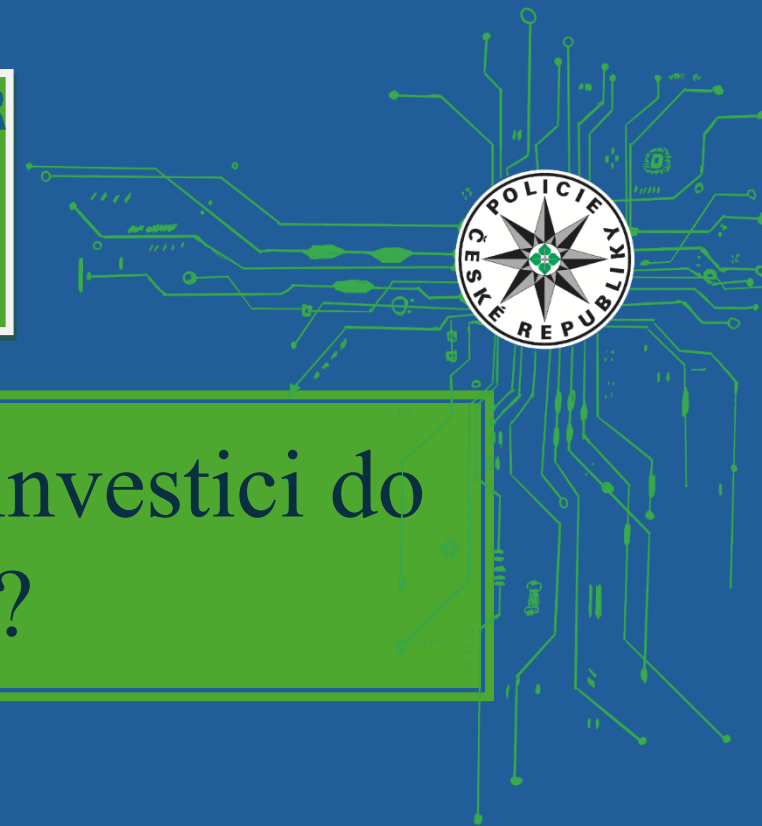
- a) Vezmu si půjčku dle instrukcí policisty a své peníze pošlu na cizí, ale technicky zabezpečený účet.
- b) Jelikož mi policista zaslal na whatsapp fotografii svého služebního průkazu, předvolání a pracovník ČNB taktéž, tak není pochyb o tom, že musím jednat, jak říkají.
- c) Ověřím si zavoláním zpět do banky, svému bankovnímu poradci, zda se tato informace zakládá na pravdě. Rozhodně si žádnou půjčku nevezmu a nikam peníze neodesílám, jelikož se jedná o podvodné jednání využívající spoofing telefonního čísla. Policista by nikdy nezasílal svůj služební průkaz jako fotografii a jednal by se mnou osobně.
- d) Půjčku si nevezmu, jelikož by mi jí nedali, ale veškeré své peníze vyberu a předám pracovníkovi ČNB u bankomatu.
- e) Jelikož mi po hovoru s policistou volali z telefonního čísla České národní banky, tak všemu věřím a radši rychle provedu.
- f) Vše provedu, a když mi volají z mé banky, že chci odeslat vysokou částku ze svého účtu a není to bezpečné, tak radši poslechnu policistu a jdu vybrat peníze z účtu a předám je pracovníkovi ČNB osobně.

Spoofing ID volajícího - Oblíbeným druhem spoofingu využívaným při vishingu je maskování čísla volajícího. Maskování může mít podobu čísla organizace, jednotlivce, konkrétního regionu podle předvolby apod. Jakmile dojde ke spojení hovoru, snaží se podvodníci získat citlivé údaje, čísla karet či přístup k bankovním účtům. Podobně může spoofing proběhnout u SMS zpráv. Útočníci k zamaskování používají specializované online služby. Instituce jsou proti podobnému útoku na jejich zákazníky prakticky bezmocné, důležitá je proto osvěta.



8. KRYPTOMĚNY

KYBERSTEZKA S PČR



Pokud prezident ČR, Petr Pavel bude propagovat výhodnou investici do kryptoměn, budete také investovat do kryptoměn, nebo akcií?

- a) Samozřejmě, když se to říká prezident republiky
- b) Bude se mi to zdát divné, ale prověřím si další videa, a když najdu propagovat výhodné investice i Andreje Babiše, tak investici provedu
- c) Nemám peníze, tak si je půjčím a budu spoléhat na to, že mi v případě podvodu Petr Pavel a policie pomůžou
- d) Zeptám se mého souseda, který také investuje, a následně investuji
- e) Uvědomím si, že politici ani veřejně známá osoba nebudou lákat na výhodné investice online, bude se jednat o podvod využívaný úpravu videa díky umělé inteligenci-deepfake
- f) Do investice přiberu celou rodinu, abychom vydělali peníze všichni a protože nevíme, jak investici provést, tak pomocí aplikace pro vzdálený přístup (např. Any Desk) nechám cizího pracovníka investic obsluhovat mé bankovníctví.

*Video o deepfake
se známými osobnostmi*



- Uvědomte si, že i když není investice přímo podvodná, tak vždy nese nějaké riziko.
- **Nikdy neumožňujte vzdálený přístup do Vašeho zařízení nikomu, koho přímo neznáte.**
- Nikdy při investování nesdělujte citlivé údaje z Vašeho bankovníctví, nebo k Vaší platební kartě.
- Nenechte se zlákat psychologií lákavých investic.
- Pečlivě si při investování čtěte podmínky.
- Na nabídky přes telefon raději vůbec nereagujte a zavěste.

Jestli chcete skutečně investovat, tak vždy s rozumem a rozvahou. Vybírejte si raději renomované společnosti a nikdy zcela nevěřte recenzím.

9. BÍLÝ KŮŇ

KYBERSTEZKA S PČR



Na internetu najdete inzerát na rychlý výdělek spočívající v přeposílání peněz přes svůj soukromý účet na jiné i zahraniční účty, co uděláte?

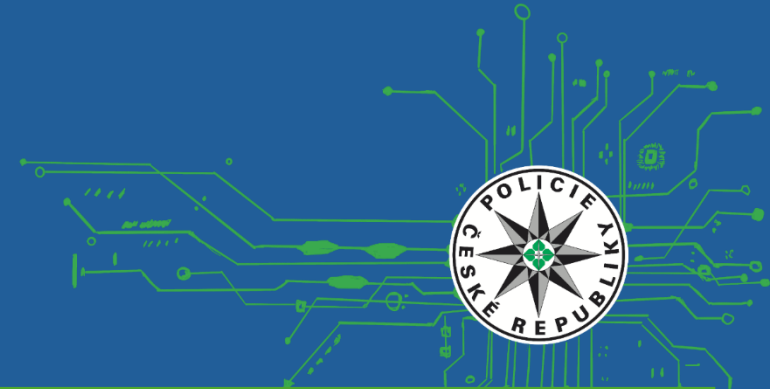
- a) Peníze potřebuji, takže nabídku příjmu a z každé přeposlané částky si budu moct nechat nějakou část pro mou potřebu. Nic nelegálního v tom nevidím. Je mi jedno, odkud peníze pochází.
- b) Zjistím, jakou částku mi dotyčný nabízí, a když to bude alespoň 1.000,-Kč za jeden převod, tak si začnu takto přivydělávat.
- c) Nechci být zatažen do praní špinavých peněz, stát se „bílým koněm“ a riskovat trestní stíhání pro legalizaci výnosů z trestné činnosti, tudíž na tento inzerát neodpovím.
- d) Přepošlu peníze jen párkrát, aby částka za mojí odměnu nepřesáhla 10.000,-kč, čímž se vyhnu veškerým možným postihům.
- e) S mým účtem si můžu dělat cokoliv a nikdo mi nedokáže, kam a proč jsem peníze posílal. Přivýdělek příjmu.
- f) Nechci se stát „bílým koněm“ a být trestně stíhaný, ale peníze potřebuje každý, takže vše budu dělat tajně. Částky budu ze svého bankovního účtu vybírat z bankomatu ihned po obdržení a pak vkládat na účty přímým vkladem. Odměnu si budu nechávat v hotovosti.

Kdo je bílý kůň? Bílý kůň je osoba, která na jinou osobu převádí peníze přijaté od třetí strany

Video o praní špinavých peněz



10. KYBERGROOMING



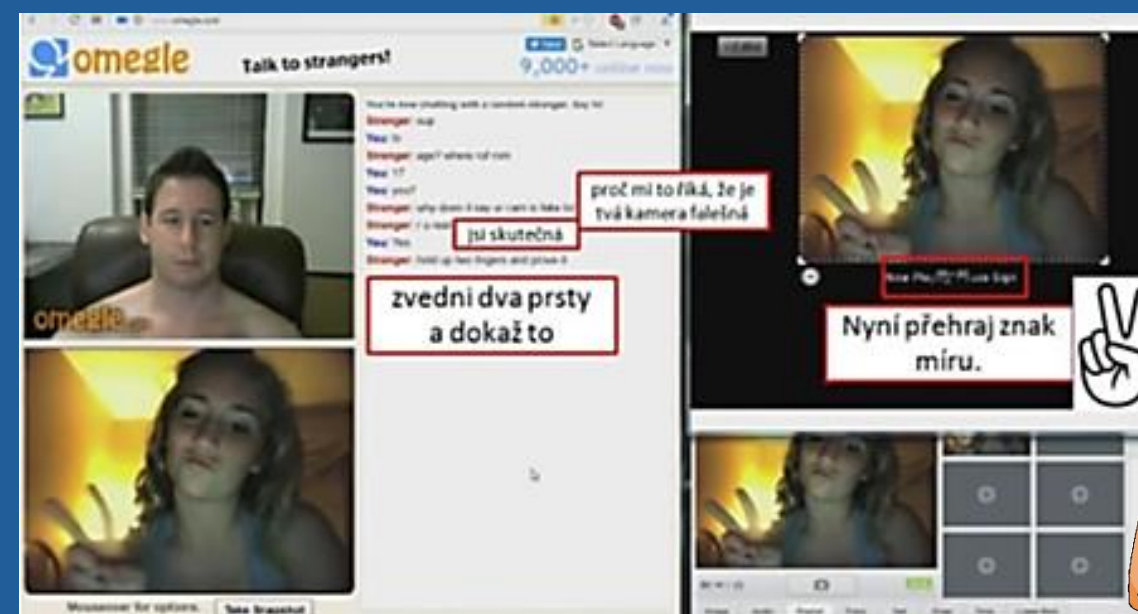
Při hraní hry vás osloví virtuální „kamarád“, kterého jste nikdy neviděli. Půjdete na schůzku? (vezměte v potaz následující informace)

Máte společné zájmy a začnete komunikovat mimo hru. Postupně zjistí, kde bydlíte, kam chodíte do školy, nebo práce. Jaké máte telefonní číslo. I když mu nepošlete intimní fotky, které po vás chce, po čase se s vámi chce setkat.

- a) Viděli jsme se na videochatu, je mi sympatický, takže půjdu. Kamarádům o tom neřeknu.
- b) Neprozradím žádné osobní informace a na schůzku nepůjdu. Mohl by to být úchyl.
- c) Vezmu kamarádku s sebou, kdyby něco, ve dvou si poradíme.
- d) Pošlu kamarádce svou polohu přes WhatsApp, rodičům ale nic neřeknu.
- e) Rodiče mě varovali před cizími lidmi na ulici, ale na internetu to je jiné.
- f) Na videu jsem ho viděla, takže vím, že je to on, a setkám se s ním.



Ke komunikaci je již využívána i v rámci videochatů umělá inteligence a nikdy si nemůžete být jistí, kdo s Vámi doopravdy komunikuje



11. ROMANCE SCAM



Na internetu vás osloví voják a ocitnete se v následující situaci, co uděláte?

V on-line prostředí vás osloví voják na zahraniční misi s romantickými zprávami. Následně za vámi bude chtít přijet, avšak bez vaší finanční pomoci, aby měl na cestu, nebo byl uvolněn z mise, se neobejde. Pod příslibem velké lásky, po vás bude chtít poslat peníze na bankovní účet, aby s vámi mohl strávit zbytek života. Jak se zachováte?

- Miluje mě, psal mi to. Jasně, že mu peníze pošlu, abychom se mohli poprvé vidět a žít spolu šťastně až na věky.
- Prověřím si, zda takový voják existuje a následně mu peníze pošlu.
- Uvědomím si, že jeho historka a sliby jsou nesmyslné. Nikdy jsem ho neviděla a nebudu posílat peníze cizímu člověku. Je mi jasné, že ze mě chce jen vylákat peníze.
- Několikrát si s ním zavolám přes video hovor, a když si budeme rozumět, tak mu peníze pošlu.
- Vyrazím na cestu za mou láskou na zahraniční misi a s cestou do Čech mu samozřejmě pomůžu.
- Jelikož jsem ho nikdy neviděla, tak mu pošlu jen peníze na uvolnění z mise a náklady na cestu si bude muset zaplatit sám.

JAK TO POZNÁM?



Někdo, s kým jste se nedávno setkali online, vám vyzná silné city a požádá vás o soukromý chat.



Jejich zprávy jsou často chybně napsané a jsou nekonkrétní.



Jejich on-line profil neodpovídá tomu, co vám říkají.

Mohou vás požádat o zaslání vašich intimních fotografií nebo videí.



Nejdříve získají vaši důvěru. Potom vás požádají o peníze, dárky nebo o údaje k vašemu bankovnímu účtu/kreditní kartě.

Pokud peníze nepošlete, mohou se vás pokusit vydírat. Pokud je pošlete, budou žádat o další.



Videa a články k romance scam podvodům



12. NEBEZPEČNÉ VÝZVY

KYBERSTEZKA S PČR



Na TikToku jste našli výzvu („challenge“) a protože se snažíte zapůsobit v kolektivu, nebo na dívku tak se na video podíváte, co bude následovat?

- a) Uvědomím si, jak je výzva hloupá. I přes naléhání svých vrstevníků mám vlastní rozum a nechci si ublížit. Nebudu se chovat jako ovce, tak výzvu rozhodně nebudu zkoušet.
- b) Když výzvu vyzkouší kamarádi, tak já taky a je mi jedno co se mi stane. Rodiče mi v případě úrazu určitě pomůžou.
- c) Abych nebyl za blbce před kamarády, tak výzvu zkusím někde v soukromí a natočím si jí.
- d) Jelikož jsem hrdina a třídní šašek, tak výzvu zkusím jako první. Jsem nesmrtelný, stejně jako postavičky ve videohrách a tudíž můžu zkoušet cokoli.
- e) Výzvu zkusím před kamarády a ponesu případné zdravotní následky, kterých si jsem vědom.
- f) Na začátku každého videa je upozornění, pokud by šlo o něco nebezpečného. Tady varování nebylo, takže výzvu vyzkouším.

Článek k nebezpečným výzvám

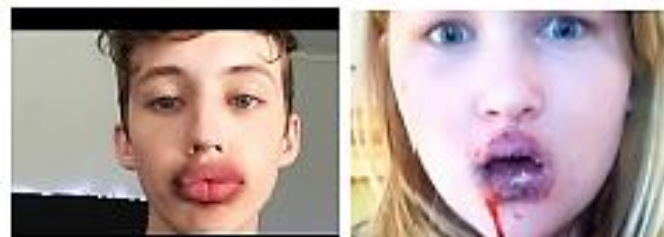


V prostředí internetu se setkáváme s velkým množstvím výzev (tzv. challenge), které **nabádají k často nebezpečnému chování, které může způsobit uživatelům internetu (především dětem a dospívajícím) vážnou zdravotní újmu.**

Online výzvy uživatele často nutí k **zapojování se do nebezpečných úkolů**, u jejichž plnění se uživatelé fotí či natáčejí, výsledek sdílejí a motivují tak další online diváky k zapojení se.

Kylie Jenner Lip Challenge

Výzva nabádá k tomu, aby si děti po vzoru modelky Kylie Jennerové zvětšovaly rty, a to tak, že si k ústům přiloží láhev, ze které odsají vzduch a podtlakem dosáhnou dočasného zvětšení rtů. Hrozí riziko poškození rtů – popraskání, krvácení apod.



Salt and Ice Challenge

Výzva, ve které si dítě či dospívající posype část těla solí a položí na ni led. **Dojde k velice bolestivé reakci a poškození a zjizvení kůže.**

Voda totiž mrzne při 0 °C, pokud ale přidáme sůl, bod mrazu se sníží až o 28 stupňů. Výsledkem této reakce jsou pak **puchýře, omrzliny, popáleniny.**



13. FAKE FIRMA



Stala se mi následující situace, porad'te mi co jsem mohl udělat jinak?

Sháním zimní pneumatiky na internetu a jedny výhodně najdu na bazaru s odkazem na známou firmu – prodejce Elite Cargo. Přes odkaz v inzerátu na e-shopu tedy pneumatiky objednáám, protože má firma výborné recenze, Podle vystavené faktury odešlu ze svého bankovní peníze. Ani po měsíci jsem však pneumatiky neobdržel, odkaz na webové stránky Elite cargo již nefunguje a je mi jasné, že jsem se stal obětí podvodu.

- a) Nic, vše jsem udělal správně.
- b) Objednat pro jistotu znovu, kdyby třeba poprvé peníze nedošli. Určitě mi přeplatek vrátí.
- c) Ověřím si hlavičku e-mailu, ze kterého mi přišla faktura, jelikož se mi zpráva nezdá. Když nezjistím nic podezřelého, tak bych dále postupoval stejně.
- d) Ověřím si, zda firma používá číslo účtu, které je uvedeno na faktuře, nebo si k číslu účtu zjistím recenze. Ověřím si hlavičku e-mailu, která je na první pohled dost podobná emailu, ze kterého komunikuje i originální e-shop. Zjistil jsem, že email není stejný, ale název odesílatele byl přejmenován. Pro jistotu zavolám do firmy podle čísla, které jsem na firmu našel, zda takové pneumatiky inzerují na bazaru. Webové stránky prověřím na **who.is**, kde se dočtu, kdy byla stránka registrována.
- e) Nemám čas kvůli pár tisícům něco prověřovat, postupoval bych stejně.
- f) Ověřím si, že firma existuje přes vyhledavač google, má sídlo firmy a více nepotřebuji. Byl jsem podveden a podám oznámení na Policii ČR, určitě peníze dostanu zpět.

Článek k podobným



Prevence: Jedinou obranou je prevence- všimnout si podezřelých znaků jakými může být třeba i nízká cena, ale i uživatelské recenze a možnost platby za požadované zboží či žádosti o vyplnění platebních údajů. Doporučujeme, prověření e-shopu na seznamu rizikových e-shopů na www.coi.gov.cz a na stránkách who.is, nebo nic.cz , kdy byla webová stránka založena.



14. REVERZNÍ INTERNETOVÉ PODVODY



Prodáváte boty na marketplace na Facebooku a kontaktuje vás zájemce s následující nabídkou, je toto jednání v pořádku?

Nabízí, že koupí boty přes Zásilkovnu. Tvrdí, že zajistí vyzvednutí, zabalení i doručení a k tomu postačí váš telefon a e-mail pro zadání údajů do aplikace. Následně vám přijde e-mail údajně od Zásilkovny s odkazem na platební bránu, kam máte pro příjem peněz zadat číslo platební karty, nebo se přihlásit do elektronického bankovníctví.

- a) Konečně kupující, který všechno zařídí, a já jen zadám svoje citlivé údaje. To je ta nejlepší služba!
- b) Zásilkovna běžně posílá odkazy, kde si zadáte platební kartu. Co by se mohlo stát?
- c) Jasně, přihlásit se přes e-mail do bankovníctví – to je přece úplně normální! Všichni to dělají.
- d) Když zadám číslo karty a odešlu, určitě mi hned přijdou peníze, že? Tohle zní jako dokonalý obchod.
- e) Je to tak pohodlné. Stačí dát někomu cizímu svoje osobní údaje a peníze jen přitečou. Takhle by měl probíhat každý obchod!
- f) Ne, toto jednání je podezřelé. Nikdy bych neměl zadávat platební údaje nebo se přihlašovat do bankovníctví přes neověřené odkazy. Pokud si nejsem jistý, vždy si ověřím, že e-mail a odkaz jsou legitimní.

Video Policie

Varování o podvodech



Odkazy nám umožňují pohodlný pohyb po internetu, bez nich by fungoval těžko. Odkaz můžeme vložit do obrázku nebo třeba slov textu-když na ně někdo klikne, odkaz ho „odvede“ na námi určenou adresu.

Stejně jednoduše je však možné odkazy zneužít a odkázat nás na nějaký škodlivý cíl. Pokud na odkaz najedeme myší a nebudeme na něj klikat, dokážeme zjistit, na jakou adresu vede, tedy odhalit jeho skutečný cíl.



15. ZAPOMENUTÉ BITCOINY



Dostanete e-mail, že Vám našli starou zapomenutou peněženku s bitcoiny. Stačí se přihlásit přes přiložený odkaz a zaplatit malý poplatek za obnovení přístupu. Poté vám bitcoiny vrátí. Co uděláte?

- a) Určitě, kdo by si pamatoval svoje bitcoiny? Zadám údaje a zaplatím poplatek, ať to mám rychle za sebou a peníze na účtu.
- b) Super nabídka! Malý poplatek za bohatství? To беру hned!
- c) Přihlašování přes náhodné e-maily a platby předem jsou přece úplně normální. Žádný problém!
- d) Nikdy nezadávám přihlašovací údaje ani neplatím poplatky přes nevyžádané e-maily. O své bitcoinové peněženice bych věděl. Je to podvod!
- e) Poplatek hradit nechci. Zadám své údaje k platební kartě, aby mi bitcoiny poslali bez úhrady poplatku.
- f) Poplatek je maličkost, když mi někdo připomene, že jsem bohatý

Doporučení:

- Nereagujte na telefonní hovory, které Vám nabízí možnost zhodnocení vašich peněz, snadný výdělek či jakýkoliv převod bitcoinové měny
- Neinstalujte si do svého zařízení žádné neověřené programy, které vám nabízí neznámá osoba pod záminkou investování.
- Nikdy na žádost neznámé osoby neklikejte na zaslaný odkaz.
- Nepotvrzujte bankovní transakce, které vám někdo nadiktuje nebo je po Vás žádá.
- Nezasílejte cizím osobám fotokopie vašich osobních dokladů.

Video k nejčastějším
Kryptoměnovým podvodům



16. VÝHODNÉ NABÍDKY



Na webu např. “Zalando na dobírku“ jste zakoupili oblečení za nízkou cenu, ale obdrželi jste levné, neznačkové oblečení. Co uděláte?

- a) Čekám na odpověď od zákaznické podpory a doufám, že to vyřeší.
- b) Kontaktuji zákaznickou podporu, ale nevěnoval(a) jsem pozornost recenzím. Pokusím se vyřešit problém.
- c) Po přečtení recenzí zjišťuji, že web je podvodný. Ohlásím to na policii a pokusím se získat zpět své peníze.
- d) Příště budu opatrnější. Reklamaci zkusím, ale příliš to neřeším.
- e) Myslím, že se jedná o chybu. Zkusím objednat znovu a budu doufat, že to bude lepší.
- f) Nechám to být. Možná jsem si špatně vybral(a), ale příště budu objednávat z důvěryhodnějších stránek.



Prevence: Vždy věnujte pozornost tomu, kde nakupujete a zda jste si jistí, že se jedná o důvěryhodný internetový obchod. Před nákupem na internetu berte v úvahu, že internetový obchod lze zřídit téměř odkudkoliv na světě během několika okamžiků, často zcela anonymně. Věnujte pozornost historii obchodu, kterou si můžete ověřit na www.nic.cz/whois/. Údaje o vlastníkově domény nemusí být pravdivé, a pokud byla doména registrována před krátkou dobou, měli byste zpozornět. Čtěte recenze o obchodníkovi, zejména ty negativní. Nápadně nízké ceny než u konkurence? Proč asi? Zkontrolujte, zda má obchod veřejně obchodní podmínky a jaká je možnost odstoupení od smlouvy.

Článek E-bezpečí

k riziku
nakupování
v e-shopech



Varování Policie

před podvody a
výhodnými
nabídkami



KYBERSTEZKA S PČR

Děkujeme, že jste se zúčastnili!



Naučte se,
jak nenaletět!



www.kybertest.cz



