

Jakkoliv to zní neuvěřitelně, lidé jsou tak zmanipulováni, že podvodníkům autorizační kódy předávají. Pachatelé díky vzdálenému přístupu do počítače oběti a přihlášení se do internetového bankovníctví mohou zcela převzít její účet, když oběť autorizuje i změnu autorizačního zařízení. Pak si již podvodníci autorizace provádějí sami a na účtu oběti si sjednají i půjčku, kterou následně odcizí. Kvůli tomu, že jim oběť umožní pod jejich smyšlenou legendou vzdálený přístup do svého počítače a přihlásí se do svého internetového bankovníctví, přijde oběť o všechny své finance a často jí ještě vzniknou dluhy.

#### 4 Firma mění číslo účtu

Čtvrtým příkladem podvodu je situace, kdy pachatel překoná bezpečnostní opatření a tím získá přístup k počítačovému systému, a tak je schopen sledovat e-mailovou komunikaci mezi dvěma firmami. Ve správný okamžik vystoupí jako jedna ze stran a kontaktuje podvrženým e-mailem obchodního partnera s

tím, že mění své číslo účtu a podvrhne pozměněné faktury k zaplacení. Aby vystupoval jako obchodní partner mu stačí nepatrná změna v podvrženém e-mailu, třeba v přidání tečky.

Obecně lze říci, že internetová kriminalita je cílena na všechny, neexistují rozdíly mezi městy, obcemi či vzdělaností. První část komunikace s obětí je vytvořena počítačovým programem, který automaticky posílá např. hromadné zprávy. Takto obešle stovky lidí s tím, že někdo jistě zareaguje. Komunikace pak probíhá telefonicky či přes Whatsapp.

#### Ztráty jdou do milionů korun

V minulém roce jsme evidovali případy, kdy oběť přišla o finanční částku přesahující v jednom případě 10 milionů a v druhém 13 milionů korun, a to v případě firem. U občanů jsme evidovali největší škodu při investování do akcií, a to přes 2 miliony korun v jednom případě a v dalším případě přesahující 1 milion korun. V desítkách dalších případů pak začínají částky od několika desítek tisíc korun až po několik set tisíc korun.

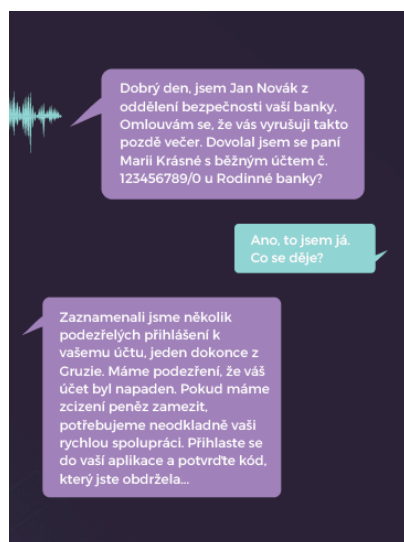
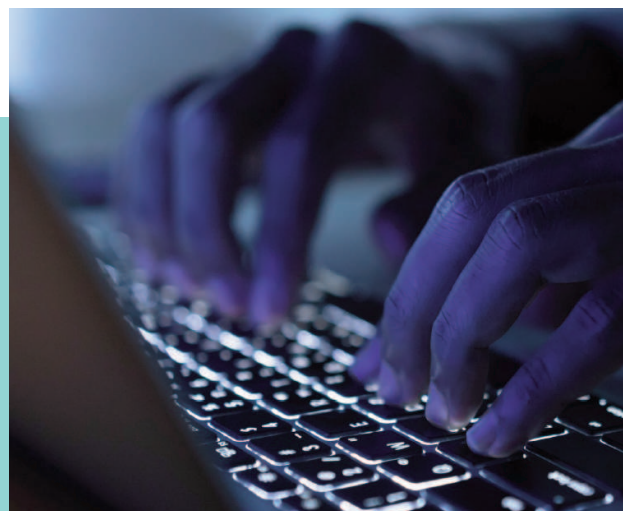
Například při prodeji litých kol na auto přišel prodejce o více jak sto tisíc korun. Při podvodném napadení účtu přišel majitel účtu o více jak tři sta tisíc korun, při investování do akcií přišel zájemce o půl milionu korun a tak dále.

#### Kdo je „legalizátor“?

Podvodně získané finance končí na tuzemských či zahraničních účtech, jsou převáděny na kryptoměnu nebo vybrány z bankomatu tzv. legalizátory, což jsou lidé například najímání přes inzeráty na tzv. rychlou brigádu. Legalizátor buď poskytne svůj účet, na který podvodník pošle pod různými nesmyslnými legendami peníze a chce, aby je přeposlal dále, vybral či vložil do bitcoinů. Legalizátor může být i zmanipulovaný člověk, který si myslí, že investuje a při tom legalizuje jinde odcizené finanční prostředky a zároveň přichází i o svoje finance. Někteří legalizátoři mají za úkol zakládat bankovní účty a přihlašovací údaje předávat podvodníkům, kteří pak účty zneužívají pro trestnou činnost. Pachatelé podnikají všechny kroky, aby se peníze ztratily a byly nedohledatelné.

## Na co si dát pozor?

- **Při prodeji nikdy nereagujte na zasláný odkaz a nepřihlašujte se v něm do své banky.** Prodejci maximálně pošlete své číslo účtu. Všechny jiné požadavky jsou nesmyslné (proč bych se při prodeji přihlašoval do svého internetového bankovníctví) a směřují k jedinému – podvodu a zisku vašich peněz.
- **Pokud volá bankéř či policista s výstrahou, že máte napadený účet a musíte vybrat peníze, jedná se o podvod!** Vždy si ověřte stav svého účtu ve své bance. Zajděte na kamennou pobočku nebo zavolejte na linku své banky. A když už si peníze vyberete a máte je v bezpečí u sebe, jaký je důvod vkládat je pak ihned do bitcoinu?
- **Osloví-li vás někdo k investici do kryptoměny či nákupu akcií, nikdy mu neumožněte vzdálený přístup ke svému počítači.** Máte-li potřebu investice či nákupu akcií, řešte to se svojí bankou na kamenné pobočce nebo s ověřenou společností s referencemi.
- **Změnu čísla bankovního účtu si ověřte.** Jestliže vám obchodní partner sdělí e-mailem, že mění číslo svého účtu, kam máte zaplatit za odebírané zboží, vždy si pro jistotu ověřte, zda komunikujete se skutečným obchodním partnerem, a že skutečně mění své číslo účtu pro platby!



Internetová kriminalita skýtá spoustu nástrah, proto buďte obezřetní a vše si pořádně rozmyslete anebo se před úkonem informujte u dotčených institucí nebo u někoho zkušeného. Jeden špatný klik vás může připravit o vše.

Pokud se přihlašujete do své banky, nikdy to nedělejte přes vyhledávač. Evidujeme případy, kdy se oběť přihlásila na stránky banky, které si našla cestou vyhledávače, ale ten ji nenašel oficiální stránky skutečné banky, nýbrž stránky podvržené, falešné s malou nepatrnou změnou v doméně. Při takovém přihlašování se tyto falešné podvržené stránky začnou „aktualizovat“ a následně vyzvou k opakované autorizaci. A to proto, aby šlo pokračovat, avšak provedenou autorizací majitel účtu pustí pachatele na svůj účet a pak i potvrdí odchodí platby z účtu.

Všechny podvržené stránky jsou vytvořeny velice kvalitně a běžný uživatel je jen stěží na první pohled rozliší. Domnívá se tedy, že jde skutečné stránky, jako například v případech odkazů z MPSV (ministerstvo práce a sociálních věcí), třeba s informací, že vám posílají peníze, ovšem s podmínkou, že až se přihlásíte do své banky, pošlou vám příslušnou platbu na váš účet. Tento požadavek je nesmyslný a jeho účelem je také odcizení všech peněz z vašeho bankovního účtu.

Při autorizaci své platby v internetovém bankovníctví vždy a raději dvakrát zkontrolujte, co autorizujete. Z případů je zřejmé, že lidé se nedívají, co autorizují a výsledkem jsou odcizené peníze, často všechny životní úspory, případně i státní dluhy a oči pro pláč.