OCHRANA OSOBNÍCH DAT A SOUKROMÍ

V příběhu...

Jarmil seděl u počítače, na kterém měl otevřený Messenger. Najednou mu přišla žádost o přátelství od jeho známé, Dajany Čudilové. Bylo mu to sice trochu divné, protože už v přátelích Dajanu měl, a to i se stejnou fotografií, nicméně přátelství potvrdil. Dajana se okamžitě zeptala, jak se má. Jarmil odpověděl, že to celkem jde.

„Jaké máš číslo mobilního telefonu?" chtěla vědět Dajana. Jarmil si pomyslel, že mu chce asi zavolat, a číslo jí poslal.
„U jakého operátora jsi?" zajímala se vzápětí Dajana.
„U H²Ofone," zavtipkoval Jarmil.
„Mám teď problém s mobilem a potřebuju pomoct. Pomůžeš mi?" poprosila Dajana.
„No jasně, tobě rád pomohu," odpověděl Jarmil.
„Teď ti přijde SMS a já potřebuju, abys mi poslal její text. Potřebuju vědět, jestli se text zobrazuje celý," pokračovala Dajana.
„OK," souhlasil Jarmil.

Vzápětí dorazila SMS. Jarmil ji bezmyšlenkovitě přepsal a odeslal. Dajana ani nepoděkovala a přestala komunikovat.

Zanedlouho zjistil, že mu z jeho účtu odešlo více než dva tisíce korun. Po chvilce přemýšlení si vzpomněl, že se to stalo v ten samý den, ve kterém si psal s Dajanou. Podíval se do mobilu na SMS, kterou si teprve teď pečlivě přečetl. Zjistil, že poslal Dajaně autorizační kód k on-line platbě. Začalo v něm růst podezření, že pěkně naletěl. Podíval se do Messengeru a zjistil, že existují dvě Dajany – Čudilová a Cudilova (bez háčků a čárek). Obě se stejnou fotografií. Navíc zjistil, že zprávy od falešné Dajany někdo vymazal a v konverzaci zbyly jen jeho odpovědi. Jarmil pochopil, že naletěl.

Nějaký zloděj si vybral Dajanu a udělal si identický profil se jménem, které bylo téměř stejné jako jméno jeho známé. Pak využil toho, že Dajana měla všechny informace veřejné, a obesílal všechny její přátele za účelem podvodu. No a minimálně u Jarmila mu to vyšlo.

Známe zásady ochrany osobních údajů (především hesla) v digitálním prostředí. Víme, jak používat a sdílet osobní identifikační údaje, abychom se vyhnuli negativním a nežádoucím důsledkům. Věnujeme pozornost bezpečnostním opatřením, spolehlivosti a soukromí.

POPIS KOMPETENCE

Dbáme na ochranu našeho soukromí a dat a uvědomujeme si rizika digitálního prostředí. Věnujeme pozornost bezpečnostním opatřením a spolehlivosti. Citlivější data chráníme dostatečně silným heslem (neodvozujeme ho od osobních údajů, pro různé přístupy volíme různá hesla) nebo jinými metodami (otisk prstu, PIN, zašifrování samotného obsahu). Své přístupové údaje nikomu nesdělujeme. Uvědomuje si, že ostatní uživatelé nemusí sdílet svoji pravou totožnost (vydávání se za jiné pohlaví, uvádění nepravdivého věku apod.), a tudíž sami nesdělujeme svoje důvěrné údaje neznámým osobám nebo uživatelům na sociálních sítích. Data, o která nechceme přijít, si pravidelně zálohujeme.

NEJČASTĚJŠÍ ČINNOSTI

Odesílání či přijímání zpráv (SMS, e-mail, chat)

Komunikace probíhá mezi jednotlivci či ve skupině (hromadné zprávy). Odesílání či přijímání zpráv lze uskutečnit pomocí mobilních telefonů či počítačů. Lze odesílat textové i obrázkové zprávy. Zprávy se předávají za účelem informování – kdy, kde a co (např. předání informací o akci, pozvánka na výlet), za účelem vzdělávání a výchovy (postup, jak nastavit mailový účet v mobilu, zaslání receptu na svíčkovou), za účelem někoho přesvědčit, motivovat (informace o společné dovolené), za účelem zábavy (vtipné SMS, společné fotografie z cest atp.).

Práce na internetu

Jedná se o jakoukoliv činnost na počítači, tabletu, mobilním telefonu apod., která vyžaduje připojení k internetu. Nejčastěji se jedná o vyhledávání informací (např. za účelem vzdělávání či zábavy), spolupráci na sdílených dokumentech, práci s online aplikacemi např. online bankovnictví, hry), komunikaci (např. domlouvání schůzky prostřednictvím messengerů, sociálních sítí, online hovorů) atd. K práci na internetu je zpravidla potřeba internetový prohlížeč.

Vytvoření a správa uživatelského účtu, nastavení uživatelských oprávnění

Uživatelským účtem se v počítačovém systému rozumí virtuální prostor vyhrazený pro činnost konkrétního uživatele. V rámci tohoto prostoru má uživatel přístup k datům a službám podle

nastavení svých přístupových oprávnění. Pro vytvoření uživatelského účtu s vyšší než základní úrovní oprávnění je zapotřebí souhlasu jiného uživatele, který již vyšší úrovní oprávnění pro správu přístupů disponuje.

ÚROVNĚ KOMPETENCE

0 –

1 Zná základní způsoby ohrožení osobních informací. Ví, že nemá mít jedno heslo pro přístup do všech digitálních aplikací, které používá. Při užívání internetu neotvírá materiál s pochybným obsahem (reklamy, nevyžádaná pošta…). Přístup do svých zařízení chrání heslem (nebo jinou formou identifikace – PIN, otisky prstů, rozpoznání obličeje).

2 Heslo nemá odvozené od osobních údajů a používá kombinaci různých znaků (malá, velká písmena, číslice, speciální znaky). Neposkytuje nikomu své přístupové údaje. Uvědomuje si, že ostatní uživatelé nemusí sdělovat svoji pravou totožnost (vydávání se za jiné pohlaví, věk apod.). Nesdílí své důvěrné údaje na internetu nebo na sociálních sítích.

3 Citlivá data šifruje (nejsou čitelná bez zadání dalšího hesla). Dokáže zvolit vhodnou bezpečnostní strategii pro sebe i domácnost, dokáže reflektovat rizika cloudových služeb, efektivně a bezpečně je využívá. Chrání svá osobní data na počítači i v mobilním zařízení (používá například antivirové programy).

DIGITÁLNÍ TECHNOLOGIE

POČÍTAČ

NOTEBOOK

TABLET

MOBILNÍ TELEFON

PERIFERIE POČÍTAČŮ – ČTEČKY KARET / OTISKŮ / JINÝCH BIOMETRICKÝCH DAT

PROGRAMY A ZDROJE

Sociální sítě • Facebook, Twitter, LinkedIn

Pomocí těchto nástrojů dnes většina lidí komunikuje se svými přáteli, rodinou nebo kolegy z práce. Lidé, volnočasové skupiny, firmy nebo neziskové organizace je používají také jako svou vizitku a místo, kde mohou rychle a jednoduše sdílet informace, pozvánku na pořádanou akci nebo zveřejnit jakoukoliv multimediální zprávu. Ke všem těmto nástrojům je třeba mít jedinečné heslo.

Nástroje pro ochranu dat a hesel

Správa hesel • KeePass, LastPass, StickyPassword

Šifrování dat • Bitlocker, VeraCrypt

Pro správu hesel a přístupů lze používat aplikace, které jedním hlavním heslem chrání seznam všech hesel. Proti zneužití dat je možné používat programy na šifrování disků, dat a dokumentů.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

MPSV

DigiKatalog | vzdělávání zaměstnavatelů a zaměstnanců v oblasti digitálních kompetencí

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

www.portaldigi.cz
Rok vydání: 2021