U KRITICKÝCH SLUŽEB JAKO ELEKTRONICKÉ BANKOVNICTVÍ, PRACOVNÍ NEBO SOUKROMÝ E-MAIL VŽDY VYUŽÍVÁM VÍCEFAKTOROVOU AUTENTIZACI.
Příkladem může být elektronické bankovnictví, kdy musím přihlášení v prohlížeči potvrdit zadáním kontrolní SMS nebo potvrzením výzvy v mém mobilním telefonu. Pokud se do služby přihlašuji z mobilního telefonu, nechám si potvrzovací SMS zaslat na jiné zařízení.

ODDĚLÍM ADMINISTRÁTORSKÝ ÚČET OD BĚŽNÉHO
Administrátorský účet používám pouze pro správu systému. Pro ostatní pracovní aktivity jako odesílání e-mailů nebo procházení webu využívám běžný neprivilegovaný účet.

NEPOUŽÍVÁM KONTROLNÍ OTÁZKY PRO OBNOVENÍ HESLA.
Nepoužívám kontrolní otázky pro obnovení hesla. Nikdy si jako alternativu k heslu nezadávám kontrolní otázky typu "příjmení třídní učitely z páté třídy" nebo “nejmenší planeta sluneční soustavy”. Podobné informace jsou dohledatelné z veřejných zdrojů. Je-li kontrolní otázka povinná, chovám se k ní jako k heslu a volím ji tak, aby nebyla dohledatelná. Např. k otázce „Jaké bylo vaše jméno za svobodna“ zvolím odpověď „N9qy$_@?9b7G&_tp“.

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

www.nukib.cz

BEZPEČNÝ POHYB V KYBERSVĚTĚ

JAK SI ZABEZPEČÍM POČÍTAČ NEBO SMARTPHONE?

OMEZÍM PŘÍSTUP DALŠÍCH OSOB K SOUKROMÝM I PRACOVNÍM ZAŘÍZENÍM.

CHRÁNÍM SVÁ DATA PRO PŘÍPAD ODCIZENÍ ČI ZTRÁTY ZAŘÍZENÍ.
Využívám silné heslo, číselný kód, gesto nebo jiný způsob zabezpečení.

NIKDY SI NEUKLÁDÁM PŘIHLAŠOVACÍ ÚDAJE K ZAŘÍZENÍM A ÚČTŮM V JEJICH BLÍZKOSTI.
Pro uchování přihlašovacích údajů používám šifrovaného správce hesel.

UJISTÍM SE, ŽE PŘI ZADÁVÁNÍ PŘIHLAŠOVACÍCH ÚDAJŮ JE NIKDO CIZÍ NEVIDÍ, NAPŘÍKLAD POHLEDEM PŘES RAMENO.

ZAMKNU ZAŘÍZENÍ POKAŽDÉ, KDYŽ OD NĚJ ODCHÁZÍM.
U počítače s Windows je nejjednodušší způsob rychlého zamknutí klávesová zkratka WIN + L a u mobilního zařízení stisknutí vypínacího tlačítka na jeho boku. Pokud odcházím na delší dobu, ukončím správce hesel a všechny doposud používané aplikace a služby s citlivými údaji jako e-mail nebo internetové bankovnictví.

AKTUALIZUJI SOFTWARE A NEVYPÍNÁM PRAVIDELNÉ AUTOMATICKÉ AKTUALIZACE SYSTÉMU.
Díky tomu zajistím opravu známých zranitelností, které by mohly ohrozit mé zařízení.

POUŽÍVÁM AKTUALIZOVANÝ ANTIVIROVÝ SOFTWARE A FIREWALL.

ZAPÍNÁM WI-FI, BLUETOOTH, NFC A DALŠÍ BEZDRÁTOVÉ TECHNOLOGIE, JEN POKUD JE VYUŽÍVÁM.
Pro útočníka představují potenciální cestu do zařízení.

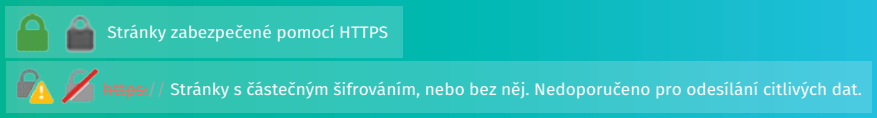
POKUD VYUŽÍVÁM NEZABEZPEČENOU WI-FI SÍŤ, VYUŽÍVÁM TZV. VPN (VIRTUAL PRIVATE NETWORK) NEBOLI VIRTUÁLNÍ SOUKROMOU SÍŤ, KTERÁ ZABEZPEČÍ MOU KOMUNIKACI NA POTENCIÁLNĚ NEBEZPEČNÉ SÍTI.

ŠIFRUJI CITLIVÁ DATA NA EXTERNÍM DISKU A DALŠÍCH PŘENOSNÝCH ZAŘÍZENÍCH.
Tak budou v případě ztráty nebo odcizení nečitelná.

PRAVIDELNĚ ZÁLOHUJI DATA.
Využít mohu například externí disk. Důležité je, aby záloha byla na jiném místě než v mém zařízení, byla šifrována a připojena pouze v okamžiku zálohování.

DO MÝCH ZAŘÍZENÍ NEPŘIPOJUJI NEZNÁMÉ USB FLASH DISKY, EXTERNÍ DISKY A JINÁ PAMĚŤOVÁ ZAŘÍZENÍ.
Mohou obsahovat malware. V případě nutnosti připojit neznámé médium provedu jeho antivirovou kontrolu. Zaměstnavatel může k tomuto účelu poskytnout tzv. antivirovou pračku, tedy počítač bez připojení k internetu, kde je nainstalovaný aktualizovaný antivirový program.

PŘI PROCHÁZENÍ WEBU PREFERUJI WEBOVÉ STRÁNKY ZABEZPEČENÉ POMOCÍ PROTOKOLU HTTPS.
Https protokol poznáme podle zámečku v adresním řádku:



DÁVÁM POZOR, NA KTERÉ ODKAZY KLIKÁM.
Je-li to technicky možné, zkontroluji, že odkaz nevede na pozdeřelou URL adresu. Pokud nemohu ověřit, kam odkaz vede, neklikám na něj.

VYPÍNÁM NEŽÁDOUCÍ SLUŽBY OPERAČNÍHO SYSTÉMU.
Například monitorování polohy, odesílání diagnostických dat, ovládání vzdáleného počítače na dálku, apod.

JAK MÁM SPRÁVNĚ A BEZPEČNĚ KOMUNIKOVAT?

K INFORMACÍM NA INTERNETU PŘISTUPUJI KRITICKY, NEMUSÍ BÝT PRAVDIVÉ.
Při práci s informacemi mohu využít rady, které sepsala iniciativa **ZVOLSI.INFO** ve svém **Surfařově průvodci internetem**.

NEZVEŘEJŇUJI OSOBNÍ ANI CITLIVÉ INFORMACE O MNĚ, MÉ RODINĚ, PŘÁTELÍCH NEBO SPOLUPRACOVNÍCÍCH.
Data narození, náboženské vyznání nebo fotografie mohou být zneužity.

INTIMNÍ FOTOGRAFIE A VIDEA NEVYTVÁŘÍM, NEUMISŤUJI JE NA INTERNET ANI JE NIKOMU NEPOSÍLÁM.
Nikdy nevím, kdy může být takový materiál zneužit.

PŘI KOMUNIKACI SI VŽDY OVĚŘUJI IDENTITU PROTISTRANY.
Mohu se zeptat přátel nebo si dotyčného vyhledat na internetu. Pokud si nejsem jist, zda mi skutečně volají například z IT oddělení naší instituce, nebo mě po telefonu úkoluje nadřízený, kterého neznám, zavěsím a zavolám zpátky na telefonní číslo z oficiálního seznamu.

NIKDY NEOTEVÍRÁM PHISHINGOVÉ E-MAILY A PODEZŘELÉ PŘÍLOHY A INFORMUJI IT ODDĚLENÍ.
V práci podezřelý e-mail neotevírám a informuji o něm IT oddělení. Stejně tak neotevírám podezřelé přílohy. Pokud mi takový e-mail dorazí do mé osobní schránky, mohu to nahlásit provozovateli schránky.

JAK PHISHING POZNÁM?
“Phishing je podvodná technika, prostřednictvím které se útočníci snaží například získat mé osobní nebo citlivé informace (přihlašovací údaje, datum narození, číslo platební karty atd.), nasměrovat mě na podvodnou stránku, nebo mi zaslat závadnou přílohu. Phishing se nejčastěji šíří formou e-mailových zpráv, které vypadají jako odeslané z důvěryhodných institucí.” Podvodník používá obecná oslovení typu „Vážený pane/í“ bez uvedeného jména, v textu e-mailu mohou být gramatické, stylistické a grafické chyby, obsahuje podezřele vyhlížející odkazy typu https://www.xbamka.cz.

V KOMUNIKACI NEJSEM ZBYTEČNĚ SDÍLNÝ.
Vše, co na sebe prozradím, může být zneužito.

NENÍ OBĚD ZADARMO A TO ANI V ONLINE SVĚTĚ.
Zpozorním, jsou-li mi zdarma nabízeny jindy placené služby nebo produkty. Pokud za produkt neplatím, jde o má data.

RANSOMWARE JE PROGRAM, KTERÝ ZAŠIFRUJE DATA NEBO CELÝ OPERAČNÍ SYSTÉM A NABÍZÍ JEJICH ZPŘÍSTUPNĚNÍ AŽ PO ZAPLACENÍ VÝKUPNÉHO.
Do zařízení se mi může takový program dostat po otevření neznámé přílohy v e-mailu, z webového prohlížeče nebo tím, že navštívím infikovanou webovou stránku. Před známými druhy ransomware mě chrání aktualizovaný antivirový program. Svá data chráním také pravidelným zálohováním.

PŘI KOMUNIKACI NESPĚCHÁM A VŠE SI PROMYSLÍM.
Útočníci rádi pracují s časovou tísní - teď je třeba něco vykonat, napravit, sdělit. Klid! Škoda z prodlení bývá menší, než důsledky neuvážených činů.

JAK ZABEZPEČÍM MÉ ONLINE ÚČTY?

PŘÍSTUPY K PRACOVNÍM I OSOBNÍM ÚČTŮM SI CHRÁNÍM SILNÝM HESLEM.
Hesla nikdy nepíšu na papírky a nenechávám například na monitoru nebo pod klávesnicí. To platí jak v kanceláři, tak i doma.

U SILNÉHO HESLA ZADÁVÁM ALESPOŇ 12 ZNAKŮ A VÍCE.
Při jeho tvorbě jsem originální a kreativní. Využívám malá a velká písmena, číslice, speciální znaky a další symboly. Mohu si zvolit například unikátní větu nebo souvětí, které si lze snadno zapamatovat.

PRO KAŽDOU SLUŽBU POUŽÍVÁM JINÉ UNIKÁTNÍ HESLO.
To platí u pracovních účtů a zařízení bez výjimky. V soukromí se této zásady držím u služeb, které mohou obsahovat osobní a citlivé informace.

NEVYUŽÍVÁM ONLINE NÁSTROJE ČI SLUŽBY PRO KONTROLU SÍLY HESLA.
Výsledkem může být to, že heslo předám útočníkovi, který si díky tomu doplní vlastní databázi používaných hesel.

PROTOŽE JE OBTÍŽNÉ ZAPAMATOVAT SI VŠECHNA HESLA, VYUŽÍVÁM PRO TA MÉNĚ VÝZNAMNÁ SPRÁVCE HESEL.
Ten mi umožňuje bezpečně uložit a spravovat velké množství hesel. Přístup do něj je chráněn jedním silným zastřešujícím heslem ideálně v kombinaci s vícefaktorovým ověřením.

NESDÍLÍM PŘIHLAŠOVACÍ ÚDAJE K VLASTNÍM ÚČTŮM A SLUŽBÁM.
V případě pracovního e-mailu, pracovního intranetu, docházkového systému nebo hesla do počítače může mít takové jednání závažné následky.