L LIMITUJTE ZDIEĽANIE

Obmedzte množstvo zdieľaných dát, či už prostredníctvom sociálnych sietí, alebo rôznych cloudových služieb. Ak niečo zdieľate, vymedzte presne osoby, ktorým zdieľané údaje sprístupníte. A po čase prehodnotíte, či zdieľanie zdroja je naďalej potrebné – a ak nie je, ukončite zdieľanie.

M MONITORUJTE

Ak sa vám stala nepríjemná udalosť v online priestore, uistite sa, že máte všetky dôkazy o bezpečnostnom incidente napr. e-maily, faktúry, potvrdenky, kópie reklamy atď. Nahláste podvod. Vaše informácie môžu pomôcť chytiť podvodníka a zabrániť ďalším incidentom.

N NEDÔVERUJTE

Mnohé z toho, s čím sa v elektronickom svete stretnete, je pochybné a nedôveryhodné. Internet je slobodným neregulovaným priestorom a každý si v ňom môže písať, publikovať a tvrdiť takmer čokoľvek. Preto je k internetovým médiám dobré pristupovať so zdravou skepsou a odstupom.

O ONLINE NÁKUPY

Skontrolujte, či sa adresa e-shopu začína na „https", a všímajte si pravopisné či gramatické chyby. Overte si, či sú v rubrikách, ako napríklad „O nás" alebo „Kontakt" uvedené legitímne kontaktné údaje. Dávajte si pozor na mimoriadne ponuky a informujte sa, aké skúsenosti majú s e-shopom iní zákazníci.

P PRIHLASUJTE SA 2-STUPŇOVO

Ak to webová služba umožňuje, používajte na prihlasovanie tzv. dvojfaktorovú autentizáciu (napríklad pomocou SMS kódu). Samotné heslo nie je už dostatočnou ochranou pred zneužitím prístupových práv.

R RANSOMVÉR JE VYDIERANIE

Ransomvér je druh malvéru, ktorý napáda počítačové systémy používateľov a zaobchádza s nimi tak, aby tieto systémy alebo dáta na nich uložené obeť nemohla (čiastočne alebo úplne) používať. Väčšinou sa to deje zašifrovaním veľkej časti údajov. Obeť zvyčajne neskôr dostane výhražnú správu, ktorá ju tlačí k zaplateniu výkupného, pokiaľ chce získať plný prístup k systému a súborom späť.

S SOCIÁLNE INŽINIERSTVO

Ľudská dôvera sa ľahko zneužíva na získanie prístupu k citlivým informáciám. Typická je forma podvodných mailov – phishing. Najlepšou ochranou pred sociálnym inžinierstvom je zvyšovanie bezpečnostného povedomia.

T TRÓJSKY KÔŇ

Škodlivý softvér, ktorý je podobný trójskemu koňovi známemu zo starovekých gréckych bájí. Aby zakryl svoju skutočnú funkciu, využíva maskovanie alebo presmerovanie. Tento malvér sa najčastejšie dostane do počítača nezodpovednosťou alebo neopatrnosťou samotného používateľa. Neotvárajte e-maily a nespúšťajte súbory, ktoré nepoznáte.

U UZAMYKAJTE ZARIADENIA

Zariadenie, ktoré nie je pod vašou fyzickou kontrolou, dáva priestor útočníkovi. Odomknuté zariadenie bez dozoru dáva komukoľvek priestor k manipulácii s ním a s jeho obsahom. Toto je potrebné uvedomiť si nielen v kancelárii, ale predovšetkým na verejných miestach (napr. na konferencii, vo vlaku a pod.).

V VZDELÁVAJTE SA

Kybernetické hrozby sú každodennou súčasťou online života, nielen v práci, ale aj v súkromí. Aby sme ich vedeli rozpoznať a účinne sa proti nim brániť, je dôležité sa pravidelne vzdelávať aj v oblasti kybernetickej bezpečnosti.

W WIFI NIE JE BEZPEČNÁ

Wifi sieť môže byť bezpečná, len ak je správne nakonfigurovaná. Nechránené wifi siete bez hesla a šifrovania sú ako dokorán otvorené dvere do bytu. Zmeňte aj pôvodný továrenský názov vášho routera a zároveň sa vyvarujte použitiu takého názvu, ktorý by vás identifikoval. Oboje totiž hackerovi zjednoduší útok.

Z ZÁLOHUJTE DÁTA

Aj pamäťové médiá sa občas pokazia a ich obsah sa stratí. Zároveň sa zvyšuje počet tzv. ransomvérových útokov, keď hackeri zašifrujú údaje a za ich vrátenie vyžadujú výkupné. Proti týmto hrozbám je účinná len obnova údajov z pravidelne vytváraných záloh.

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

CSIRT.SK

SK CERT
NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

ÚRAD NA OCHRANU OSOBNÝCH ÚDAJOV SLOVENSKEJ REPUBLIKY

AKB
Asociácia kybernetickej bezpečnosti

www.cybercompetence.sk www.csirt.gov.sk www.sk-cert.sk www.dataprotection.gov.sk www.akb.sk