Дигитална безбедност

Како да се заштитите при работа во дигиталниот свет

Размислете пред да кликнете

Сајбер криминалците често користат интересни и возбудливи теми со цел да ве намамат да кликнете на некој малициозен линк. Застанете и размислете пред да кликнете и дополнително користете bitdefender.com или kaspersky.com

Користете менаџер на лозинки

keepass.info или buttercup.pw се добри алатки за да ги чувате сите ваши лозинки на едно место, енкриптирани и заштитени. Сè што треба е да запомните само една лозинка.

Правете редовен бекап

Доколку вашиот уред престане да работи или е украден, сите податоци кои ви биле важни ќе ги изгубите засекогаш. Затоа од клучна важност е да чувате бекап на втора локација. amanda.org или backuppc.github.io се одлични софтверски решенија за таа цел.

Користете легален софтвер и редовно ажурирајте го

Користење на легален софтвер и негово редовно ажурирање ве штити од злонамерен софтвер и ја оптимизира работата на вашиот уред. Доколку сте невладина организација и ви треба легален софтвер, може да ви помогне techsoupnorthmacedonia.org

Безбеден мобилен уред

Користете лозинка, пин или друга заштита за заклучување на вашиот мобилен уред. При губење или кражба на вашиот мобилен уред, уредот можете да го лоцирате со помош на Find my iPhone, Android Device Manager или Lookout.

Не употребувајте исти лозинки

Постојаната употреба на исти лозинки секаде може да им ја олесни работата на хакерите да добијат пристап до сите ваши профили и уреди одеднаш. Користете комбинирани лозинки (голема и мала буква, симболи, бројки) или неколку неповрзани зборови со цртичка помеѓу нив.

Погледнете кој ви праќа пораки и документи на мејл

Бидете внимателни при кликнување на линкови и документи што ви се пратени, бидејќи можно е да содржат малвер што ќе му наштети на вашиот уред.

Размислете каде споделувате приватни информации

Лични и сензитивни податоци како имиња на членови од семејство, родендени, регистрација на возилото и адреса на вашето живеалиште кои ги споделувате на интернет некогаш може да бидат употребени и против вас.

Користете дво-факторска автентикација

Ова дополнително ниво на заштита драстично ја зголемува безбедноста на вашите профили. Насоки за активирање на 2FA постојат на веб-сајтовите на сите поголеми сервиси како Фејсбук , Инстаграм, Gmail, Твитер и други.

Користете VPN

VPN(Виртуелна приватна мрежа) е алатка за заштита на комуникација при користење на уред на интернет. При користење на јавни мрежи секогаш користете protonvpn.com или psiphon.ca

digitalfirstaid.mk

Поддржано од The Information Safety & Capacity (ISC) Project

Реализирано од Фондацијата Метаморфозис