**domácí IT audit**

přehled základních oblastí a kroků pro zabezpečení a edukaci

# zabezpečení domácí sítě

* Domácí Wi-Fi síť je zabezpečená heslem
* Všichni, kdo mají znát heslo, jej znají, nebo vědí, kde jej najdou
* Přístup na router je chráněný vlastním heslem, nikoli heslem od výrobce
* Router má aktualizovaný firmware
* Zkontrolovat, zda neplatí za zbytečné služby, které nejsou využívány

# zabezpečení operačního systému

* Systém je aktualizovaný a jsou nastavené automatické aktualizace
* U přenosného počítače je přístup na uživatelský účet chráněn PINem a heslem
* Systém je – pokud je to vhodné – zabezpečen proti změnám ze strany uživatele (oddělení administrátorských práv)
* V systému nejsou nainstalovány zbytečné aplikace (bloatware) a není zaneřáděn nežádoucími aplikacemi (malware)
* V systému je aktivní firewall a případně antivir

# zabezpečení prohlížeče v PC

* Naistalován bezpečný a moderní prohlížeč
* V prohlížeči nejsou nebezpečné nebo zbytečné pluginy a rozšíření
* Aktivované HTTPS Everywhere apod., případně ochrana před sledováním
* Funkční správce hesel

# hesla

* Nainstalovaný a zprovozněný správce hesel
* Silná a různá hesla k nejdůležitějším službám
* Uživatel zná své hlavní heslo nebo ví, kde jej najde, je poučen o jeho důležitosti
* Uživatel vyzkouší, jak generovat nové heslo pomocí správce hesel
* Nastavena a vyzkoušena dvoufaktorová autentizace u důležitých služeb

# zálohování a vyčištění disku

* Zjistěte, zda na disku nejsou staré, duplicitní nebo zbytečné soubory a složky
* Smažte dočasné soubory, cache, nepotřebné stažené soubory, nepotřebné zálohy driverů
* Zkontrolujte, zda jsou všechny dokumenty a fotografie zálohované (externí disk, cloud)
* Nastavte automatickou zálohu nebo vytvořte plán pro pravidelné zálohování

# zabezpečení mobilního telefonu

* Aktivujte zamčení telefonu a šifrování
* Zakažte aplikacím sledovat polohu
* Zjistěte, zda nejsou na telefonu nepotřebné aplikace nebo soubory/složky
* Nastavte automatické zálohování
* Zprovozněte správce hesel
* Uživatel ví, že by neměl instalovat aplikace z neznámých zdrojů

# povědomí o riziku online

* Uživatel zná základní principy bezpečnosti na internetu a zná příklady podvodů a spamů
* Uživatel ví, že lze podvrhnout e-mailovou adresu i webovou stránku
* Uživatel rozumí tomu, že existují falešné stránky, aplikace, reklamy, recenze, profily, magazíny, falešné faktury, exekuce atd.

# nakupování a bankovnictví

* Uživatel rozumí tomu, jak přistupovat ke svému účtu a jak je zabezpečen
* Uživatel ví, že nemá posílat SMS kód od banky
* Uživatel ví o existenci podvodných e-shopů

# Vzdálená pomoc

* Uživatel ví, jak vás případně požádat o pomoc
* Uživatel ví, jak spustit program pro vzdálenou podporu (nejlépe názorná ukázka naživo)