Doporučený způsob zabezpečení (v souvislosti s GDPR)

1 Wi-Fi

Pro zabezpečení Vaší domácí Wi-Fi je vhodné použít šifrování WPA2-PSK (AES). Heslo by mělo mít přibližně 10 znaků a mělo by být co nejhůře odhadnutelné (rozhodně se vyhněte nejen jménům členů rodiny/mazlíčků, adresy bydliště, ale i heslům typu „123456789“,“heslo1234“ atd.). Pokud je Wi-Fi router někde na dosah ostatním lidem, je vhodné vypnout funkci WPS, ta umožňuje připojení Wi-Fi po pouhém kliknutí tlačítka na routeru. Pokud se na Vaši Wi-Fi připojují i cizí lidé, můžete (pokud to Váš router umožňuje) zapnout funkci Guest Wi-Fi, která odděluje hlavní síť (Vaši) od sítě, do které se připojují ostatní. Připojení k internetu funguje pro obě sítě totožně. Nikdy nenechávejte Wi-Fi bez hesla!

Veškerá tato nastavení se většinou nacházejí pod položkou Wi-Fi -> Zabezpečení

2 Telefon

V případě mobilního telefonu je vhodné mít telefon zabezpečen. Většina dnešních telefonů nabízí zamknutí telefonu na heslo či otisk prstu. Heslo k telefonu by mělo být jedinečné (ne stejné jako na PC) a pokud to telefon umožňuje, je lepší zvolit komplikovanější heslo s více než 4 znaky. Pokud je to možné, telefon mějte stále u sebe a nenechávejte ho nikde bez dozoru.

Pokud to není naprosto nezbytně nutné, vyhněte se připojování na nezabezpečené Wi-Fi, jelikož nikdy nevíte, kdo může sledovat vaši komunikaci přes internet. Pokud je to možné, udržujte Vás telefon aktualizovaný. Nejnovější aktualizace často opravují chyby v zabezpečení telefonu.

3 PC

Také na počítači je vhodné nastavit si heslo, opět by mělo odpovídat jistým pravidlům (viz. Wi-Fi). Slabé heslo se dá jednoduše prolomit.

Délka hesla	Všechny znaky	Pouze písmena (a-z)
3 znaky	0.86 sekundy	0.02 sekundy
4 znaky	1 minuta 21 sekund	0.046 sekundy
5 znaků	2 hodiny 9 minut	12 sekund
6 znaků	8 dní 12 hodin	5 minut 9 sekund
7 znaků	210 let	2 hodiny 14 minut

Tabulka znázorňující průměrnou dobu potřebnou k prolomení hesla

Pokud se od počítače vzdalujeme, je vhodné počítač zamykat. Počítač se systémem Windows můžeme zamknout přes nabídku Start -> profil -> Uzamknout. Kromě nevyhnutelných případů doporučujeme nezadávat vaše údaje na cizím PC. Také bychom měli být obezřetní, jaké stránky navštěvujeme, zda máme funkční antivir a nestahovat podezřelé soubory.

Nezapisujte si heslo na papírky na pracovním stole.

4 Šifrování

Pro zvýšení bezpečnosti našich dam, můžeme zašifrovat disk. Pokud se k šifrování rozhodnete **DOPORUČUJEME zálohovat vaše data**, jelikož v případě zapomenutí hesla se k datům již nedostanete. Pokud máte Windows 10 Pro, můžete použít nástroj BitLocker, který je ve Windows 10 předinstalovaný. Pokud hledáte alternativu zdarma, existuje nástroj VeraCrypt, ten však funguje většinou pouze s Windows 7 a nižšími.