

DESATERO BEZPEČNOSTI NA INTERNETU

1. ZABEZPEČTE SI POČÍTAČ

Nainstalujte si a pravidelně si aktualizujte antiviry a firewally na svém počítači na nejnovější verzi. Zvýšíte tím bezpečnost svých souborů, protože aktuální verze dokážou zachytit hrozby a viry, které jsou na internetu i pár dní.

2. ZABEZPEČTE SI MOBILNÍ TELEFON

Chraňte i svůj telefon. V každém mobilním obchodě s aplikacemi najdete množství bezpečnostních aplikací, které jsou dostupné zdarma nebo za malý poplatek.

3. OVĚŘUJTE SI PŮVOD APLIKACÍ

Aplikace stahujte přímo z oficiálních obchodů ve vašem telefonu (App Store, Google Play). Před stažením věnujte pozornost recenzím a hodnocení aplikace, a jestli nejste mezi prvními, kdo aplikaci stahuje.

4. CHRAŇTE SVÉ PŘIHLAŠOVACÍ ÚDAJE

Se svými přihlašovacími a osobními údaji zacházejte opatrně. Nikomu je nesdělujte, neukládejte je na počítačích ve veřejných sítích nebo ve škole, a zadávejte je jen na bezpečných serverech.

5. PIN JAKO V OKO HLAVĚ

Je váš PIN datum narození nebo 1234? Rychle si ho změňte a zapamatujte. Pokud víte, že jste zapomnětliví a musíte si PIN schovat, nenechávejte ho v blízkosti platební karty a strážte ho jako oko v hlavě.

6. MĚJTE BEZPEČNÉ HESLO

Heslo by mělo být neodhadnutelné (NE vaše jméno apod.), silné (kombinace velkých i malých písmen a znaků), nezjistitelné (např. hackerský program zkouší slova ze slovníku) a především unikátní – nikdy nepoužívejte stejné heslo pro různé služby (např. sociální sítě, e-mail a bankovní účet)! Hesla s nikým nesdílejte a neukládejte je do prohlížeče. Pokud si je nezapamatujete, запиšte si je, ale následně uložte na bezpečné místo (trezor)! Pokud je to možné, zvolte k účtům dvoufaktorové ověřování.

7. POZOR NA NEZNÁMÉ PŘÍLOHY

Pokud vám někdo pošle odkaz nebo přílohu, kterou nečekáte, buďte velmi opatrní. Tyto odkazy nebo přílohy mohou obsahovat viry (malware) nebo jiný škodlivý software, který může poškodit váš počítač nebo zneužít vaše osobní údaje. Než něco otevřete, vždy si ověřte, zda to pochází od důvěryhodného zdroje.

8. NAKUPUJTE JEN U PROVĚŘENÝCH ON-LINE PRODEJCŮ

Přes internet nakupujte u prověřených a důvěryhodných prodejců – orientujte se podle ikony zamknutého visacího zámku u URL adres jejich webu, musí být bez jakéhokoli upozornění. To samé platí u přihlašování na jakýkoli web, zejména pak pro bankovní služby! U soukromých inzerentů a méně známých prodejců čtěte recenze.

9. ČTĚTE UPOZORNĚNÍ BANKY (ESSOXU)

A nejen ty bankovní, ale také vašeho počítače. Pokud upozornění jen odklikáváte, může vám např. uniknout zpráva z vaší banky o útocích hackerů. Věnujte jim tak pozornost a chraňte sebe i svůj účet.

10. INFORMUJTE BANKU (ESSOX)

Pokud máte, byť jen podezření, že se s vaším účtem děje něco podivného či špatného, kontaktujte svou banku. Přes infolinku vám zákaznická podpora dokáže zkontrolovat váš účet, zablokovat příkazy nebo ztracenou kartu.