

## 9 KYBERBEZPEČNOSTNÍCH TIPŮ PRO ZAMĚSTNANCE

### 1. Neignorujte aktualizace

Operační systém i antivirový software byste měli aktualizovat pravidelně a pokaždé, když je aktualizace k dispozici. Většina aktualizací je vydávána k posílení bezpečnosti nebo zabránění přístupu škodlivého softwaru k vašim datům a systémům.

### 2. Budte obezřetní při otevírání e-mailů od lidí, které neznáte

Raději vícekrát překontrolujte jméno a doménu odesílatele e-mailu, jestli se opravdu shoduje s osobou v podpisu. Neklikejte na odkazy ani neotvírejte přílohy, pokud neznáte jejich původce, odesílatele nebo jste o zaslání dokumentu nežádali.

### **PxH1#n!** 3. Volte silná hesla a měňte je pravidelně

Volte hesla, která si zapamatujete, ale zároveň bude těžké je prolomit. Doporučujeme alespoň 12 znaků, kombinaci symbolů, čísel a velkých a malých písmen. Skvěle fungují třeba celé věty.

### 4. Neignorujte varování na webových stránkách

Existují nástroje a rozšíření, která za vás mohou kontrolovat odkazy a varovat před nebezpečnými webovými stránkami. Zeptejte se IT oddělení, jaké blokátory reklam nebo pluginy jsou vhodné pro vaše zařízení.

### 5. Hlaste podezřelé aktivity IT oddělení

Pokud obdržíte podezřelý e-mail a máte obavy o bezpečnost vašeho systému nebo dat, ihned kontaktujte IT oddělení. Kolegové z IT přijmou potřebná opatření a postarají se, aby vaše data zůstala v bezpečí.

### 6. Mějte na svých zařízeních minimum citlivých dat

Veškerá data, která nepoužíváte, by měla být zálohována a odstraněna z pracovních stanic, aby se minimalizoval dopad případných bezpečnostních incidentů a zajistila se ochrana dat klientů a jejich soukromí.

### 7. Nenechávejte svá zařízení bez dozoru

Nastavte pro své zařízení uzamčení obrazovky po rozumném čase nečinnosti, aby se nikdo nemohl dostat k vašim datům, pokud budete muset nečekaně odběhnout a věnovat se něčemu jinému.

### Wi-Fi 8. Vyhybejte se používání veřejné Wi-Fi

Nepřipojujte se k veřejným Wi-Fi sítím. Pokud je opravdu nutné veřejnou Wi-Fi použít, ujistěte se, že po připojení síť smažete, aby se vaše zařízení automaticky znovu nepřihlásilo, když budete v dosahu.

### **WWW.NESMYSL.CZ** 9. Ověřujte URL odkazy

Vždy zadávejte adresu své banky (nebo jiných online služeb, jako je finanční úřad) do prohlížeče sami a nikdy nepoužívejte odkazy z e-mailů nebo webových stránek k přístupu k těmto stránkám.