5 KROKŮ NA CESTĚ K BEZPEČNÝM VIDEOHOVORŮM

1.

ZKONTROLUJTE SVÉ PRACOVNÍ PROSTŘEDÍ

Během videohovorů by za vámi neměly být tabule, které obsahují důležité firemní či jinak citlivé informace. Před začátkem streamování raději vždy zkontrolujte, co mohou účastníci online konverzace prostřednictvím vaší webkamery vidět.

2.

PROJDĚTE SI NASTAVENÍ SYSTÉMU VIDEOKONFERENCE

Nastavte pro své pracovní prostředí správnou konfiguraci, abyste zajistili bezpečnou firemní komunikaci. Zkontrolujte přitom zásady ochrany osobních údajů služby, kterou právě používáte.

3.

DBEJTE NA ŘÍZENÝ VSTUP DO ONLINE HOVORŮ

Omezte přístup účastníkům z internetové domény a raději vytvářejte kontrolované skupiny uživatelů, v rámci kterých si pak budete volat. Je-li to možné, nastavte si v aplikaci pro videohovory heslo schůzky nebo číselné heslo k ověření uživatelů, kteří se připojují telefonicky. U aplikací, jako je Zoom nebo Google Hangout, udržujte účastníky v „čekárně", dokud je neschválíte.

4.

ŠIFRUJTE SDÍLENÉ SOUBORY I CELOU KOMUNIKACI

Některé služby ve výchozím nastavení automaticky šifrují chat. U videa si to ale často musíte nejprve sami manuálně nastavit. Při odesílání a přijímání souborů se vyvarujte spustitelných souborů s příponou .exe nebo .com.

5.

POZOR NA SDÍLENÍ OBRAZOVKY

I jedna ikona nebo název souboru může uživateli na druhé straně počítače poskytnout citlivé informace. Například software Apple iOS pořizuje snímky obrazovky, když dochází k přepínání mezi aplikacemi. Pokud tomu chcete zabránit, zkontrolujte, zda program pro videokonferenci může obraz na ploše rozmazat ve funkci „blur".

ZDROJ: ESET