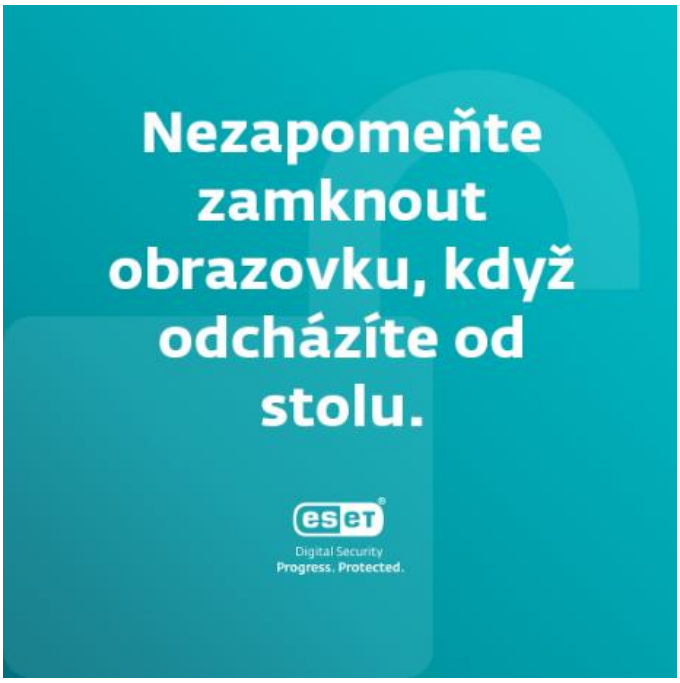


Nezapomeňte zamknout obrazovku, když odcházíte od stolu.

Zatímco někteří kolemjdoucí vás mohou chtít pouze překvapit odesláním zdánlivě vtipného e-mailu z vašeho účtu, jiní mohou hledat data, která by mohli zneužít. Chraňte citlivá data své společnosti tím, že vždy uzamknete obrazovku, když necháváte počítač bez dozoru. Zde jsou zkratky, které můžete k okamžitému uzamčení obrazovky použít:

- Stiskněte klávesovou zkratku Ctrl + Alt + Delete, a poté klikněte na UZAMKNOUT
- Stiskněte klávesu s logem Windows + L
- Stiskněte klávesy Control + Command + Q (pro MacBook)

Změňte své heslo na přístupovou frázi.

Dobré heslo je snadno zapamatovatelné, ale obtížně uhodnutelné. Čím delší, tím lepší. Nejjednodušší způsob, jak toho dosáhnout, je povýšit heslo na přístupovou frázi.

Jak si můžete vytvořit dobré heslo?

1. V ideálním případě by dobré heslo nebo heslová fráze měla obsahovat kombinaci velkých a malých písmen, číslic a speciálních znaků.
2. Zahrňte informace, které zná jen málo lidí, například vaši starou přezdívku z dětství, oblíbený film nebo interní vtip.
3. Vyhněte se informacím, které lze snadno najít, jako jsou jména vašich domácích mazlíčků nebo vaše narozeniny.
4. Některá slova nebo písmena nahraďte čísly a symboly. Místo „heslo“ zkuste „h€sL0_“.
5. Přidejte něco náhodného. Pokud zvolíte například frázi z filmu nebo text písně, pravděpodobně to už někdo udělal, což usnadní prolomení hesla. Zkuste přidat něco nesouvisejícího, co dává smysl jen vám.

Příklad:

„Opět je prosinec!“ změňte na „O5_j€_pr0s1Nec!“

Pro každý ze svých účtů používejte jedinečné heslo.

Možná si myslíte, že se nic nestane, když někdo prolomí heslo k vašemu zákaznickému účtu v IKEA. Možná máte pravdu - pokud jste tam nepoužili stejné heslo, které už používáte pro vaše ostatní účty, včetně těch pracovních. Pokud opakovaně používáte stejné heslo pro všechny účty, které máte, je pro vás možná snazší si ho zapamatovat, ale rozhodně to není bezpečné.

Věnujte nějaký čas tomu, abyste prošli své účty a změnili přihlašovací údaje tak, abyste pro každý účet používali jiné heslo.

Používejte správce hesel.

Pokud používáte bezpečné přístupové fráze nebo jedinečné heslo pro každý z účtů, může být obtížné zapamatovat si všechny přihlašovací údaje. S tím vám pomohou správci hesel. Pokud budete používat správce hesel, stačí si pamatovat pouze jedno heslo a přitom si zachováte vysokou úroveň zabezpečení. V ideálním případě můžete také zapnout MFA (vícefázové ověřování), které zvyšuje bezpečnost správce hesel. Někteří správci hesel nabízejí také speciální funkce, například ukládání důvěrných dokumentů. S výběrem a instalací bezpečného a snadno použitelného správce hesel vám může pomoci vaše IT oddělení.

Konzultujte všechny nové aplikace se svým IT specialistou.

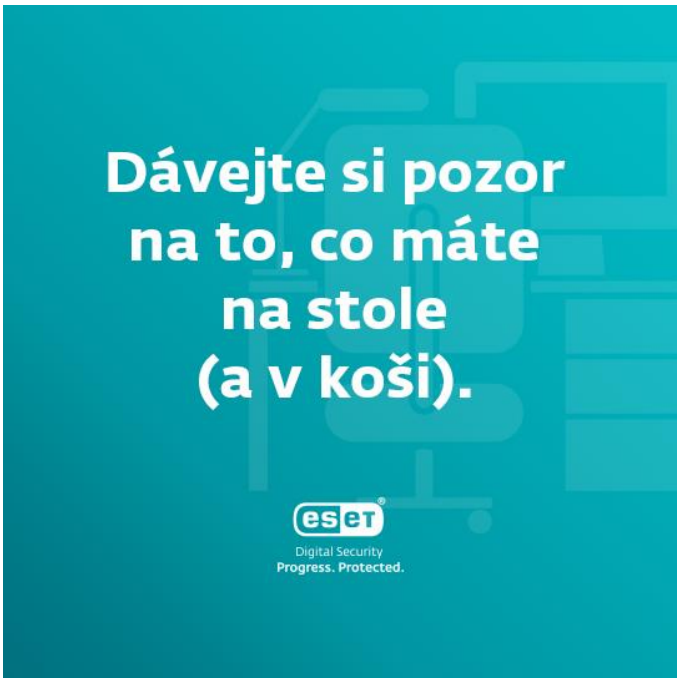
Chcete si do pracovního zařízení nainstalovat novou aplikaci? Vždy se poraďte se svým IT oddělením. To by mělo určit, zda je aplikace bezpečná - například na základě toho, jakým způsobem zpracovává data, jaký rozsah přístupů vyžaduje nebo co se stane s jejími uživateli, když přestane fungovat. Váš IT specialista vám vysvětlí, jak aplikace funguje a jak ji bezpečně používat, abyste zachovali svou vlastní i firemní digitální bezpečnost.

Dvakrát se rozmyslete, než kliknete na odkazy v e-mailech.

Seznamte se s phishingem a taktikami, které kyberzločinci používají, aby vás nalákali do svých pastí. Zde je několik příkladů. Zapamatujte si základní znaky phishingového e-mailu: obecný pozdrav, špatná gramatika, URL adresa a předmět e-mailu, které neodpovídají obsahu zprávy, pocit naléhavosti a požadavek na rychlou akci. Lidé se často nechají phishingovými e-maily oklamat, protože jednají pod tlakem. Věnujte čas opatrnému čtení e-mailů a pamatujte, že samotné otevření e-mailu je obvykle neškodné. Možné nebezpečí spočívá v neznámých odkazech a přílohách, ale také v obrázcích obsažených ve zprávě, které mohou útočníkovi umožnit odhadnout vaši polohu, informace o zařízení, operačním systému apod. Zločinec pak může tyto informace využít k budoucímu útoku na vás nebo na vaši společnost, proto je dobré zakázat automatické načítání obrázků. Pokud zjistíte pokus o phishing, vždy informujte IT oddělení.

Pokud jde o cizí lidi v kanceláři, důvěřujte, ale prověřujte.

Kdykoli uvidíte někoho neznámého, kdo se prochází po prostorách vaší kanceláře, jako by se ztratil, zeptejte se ho, zda nepotřebuje vaši pomoc. Pokud se vám zdá podezřelý, nebojte se o něm informovat ochranku. Stejně jako u jiných věcí platí, že je lepší sázet na jistotu a zůstat v bezpečí, než řešit únik dat kvůli zákeřnému narušiteli. Zdá se vám tento scénář nereálný? Přečtěte si příběh o tom, jak se Jake Moore, odborník na kybernetickou bezpečnost, v přestrojení naboural do společnosti kvůli špatné informovanosti zaměstnanců.



Dávejte si pozor na to, co máte na stole (a v koši).

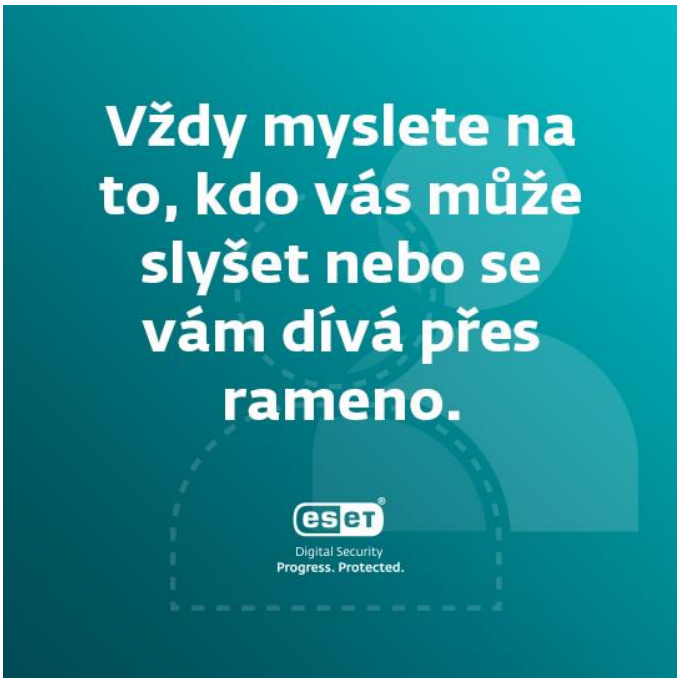
V dnešní době se více zaměřujeme na digitální data než na fyzické dokumenty. Přesto, pokud by tyto dokumenty opustily pracovní prostory a viděla je cizí osoba, může to ohrozit vaši společnost. Abyste se této situaci vyhnuli, vždy před vyhozením důvěrné dokumenty skartujte. Kromě toho nezapomínejte kontrolovat, co máte na stole. Jsou tam nějaké dokumenty, které by nikdo neměl číst? Nebo důležité poznámky, které nechcete sdílet? Raději je uložte do šuplíku a uzamkněte.

Vyhněte se připojování k veřejným sítím Wi-Fi.

Místa s veřejnou sítí Wi-Fi se zdají být atraktivní nejen pro vás, ale i pro kyberzločince. Výsledkem mohou být veřejné Wi-Fi infikované malwarem (prostřednictvím routeru), falešná veřejná Wi-Fi připojení, která byla vytvořena hackery, nebo takzvané útoky Man-in-the-Middle (MitM), během nichž se kyberzločinci umístí mezi vás a místo připojení a shromažďují vaše údaje. Pokud se opravdu potřebujete připojit k veřejné Wi-Fi, mějte vždy zapnutou síť VPN a nenavštěvujte stránky, které vyžadují zadávání vašich přihlašovacích údajů, jako je například internetové bankovnictví.

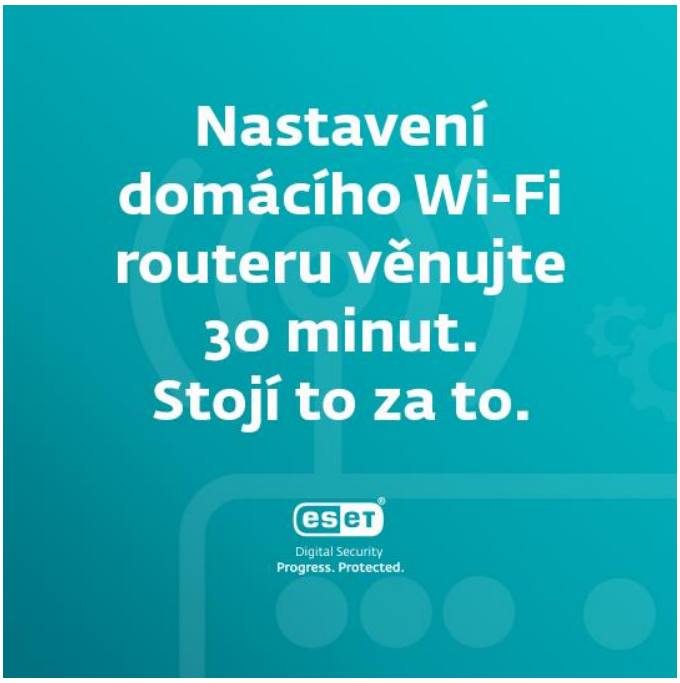
Při videohovorech a sdílení obrazovky ukazujte jen nezbytné.

Pro mnohé se videohovory staly nedílnou součástí jejich práce. Stejně jako při osobním jednání existují určitá pravidla, která je třeba dodržovat, abyste se vyhnuli jakémukoli riziku. Pokud potřebujete sdílet obrazovku, ujistěte se, že ukazujete pouze okna, která mají být zobrazena, a že na pozadí nejsou žádné soukromé dokumenty. Totéž platí i pro vaše okolí. Pokud můžete, rozostřete pozadí a vždy zkontrolujte, zda za vámi není něco, co není bezpečné sdílet - například tabule s poznámkami z interní porady.



Vždy myslete na to, kdo vás může slyšet nebo se vám dívá přes rameno.

Potřebujete se přihlásit ke svým pracovním účtům v autobuse? Nebo vyřizovat pracovní telefonát v kavárně - nebo dokonce na vlastní zahradě? Mějte na paměti, že lidé kolem vás toho mohou využít. Pokud někdo uvidí vaše přihlašovací údaje, může je použít k tomu, aby se dostal do vašich účtů, takže když jste na veřejnosti, používejte biometrické ověřování, například Touch nebo Face ID. Při práci mimo kancelář může kdokoli mimo firmu vidět, co máte na obrazovce, včetně citlivých dokumentů, proto zvažte pořízení privátního filtru pro obrazovku. Pamatujte také na to, že kdokoli může odposlouchávat vaše pracovní telefonní hovory a využívat jakékoli citlivé informace, kterou sdílíte. Vždy je lepší diskutovat o důvěrných tématech pouze tehdy, když víte, že vás nikdo neposlouchá.



Nastavení domácího Wi-Fi routeru věnujte 30 minut. Stojí to za to.

Práce z domova se pro mnohé stala standardem. Nahraďte výchozí přihlašovací údaje (včetně názvu Wi-Fi a výchozího hesla) bezpečným heslem nebo přístupovou frází, vypněte vzdálenou správu, aktualizujte firmware a zapněte šifrování sítě - ideálně WPA3. Nejste si jisti, jak to udělat? Zde je několik tipů. A pokud si stále nejste jisti, jak postupovat, vždy se můžete obrátit na své IT oddělení. Bez těchto preventivních opatření se jakýkoli vnější narušitel poměrně snadno dostane k vašim datům, a to jak pracovním, tak osobním.

Zjistěte, zda někdy nedošlo ke kompromitaci vašich přihlašovacích údajů.

Jděte na web Have I Been Pwned, zadejte svou e-mailovou adresu a zjistěte, zda vaše přihlašovací údaje byly někdy součástí úniku dat. Pokud ano, nastavte si na kompromitovaných účtech - i na všech ostatních - nové silné heslo.

Dávejte si pozor na to, co sdílíte na sociálních sítích.

Chcete sdílet selfie z kanceláře? Nebo zábavnou fotku svého pracovního stolu? Tím, že ukážete prostředí, ve kterém pracujete, můžete narušiteli usnadnit orientaci v prostoru a dát mu pocit, že tam patří. Navíc můžete nevědomky sdílet některé citlivé informace o svých spolupracovnících, zaměstnavateli nebo o sobě - například pokud fotka vašeho pracovního stolu obsahuje citlivé dokumenty nebo poznámky s přihlašovacími údaji. Než začnete sdílet cokoli, co se týká práce, ujistěte se, že to zahrnuje pouze veřejně známé informace.

Kde lidé sdílí, přátelství sílí. Ale ne, pokud jde o pracovní zařízení.

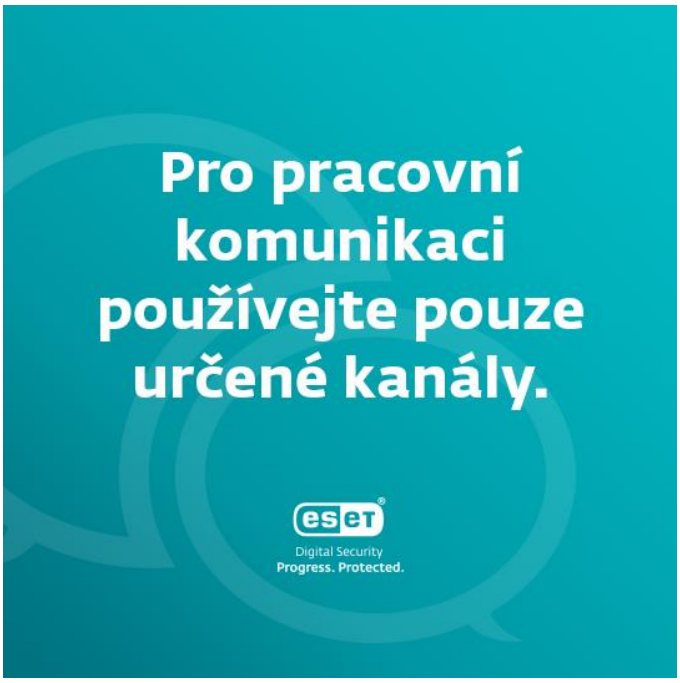
I když vás možná láká nechat děti používat váš pracovní počítač k hraní her nebo sledování filmů, vaše zařízení obsahuje data, která by neměla být sdílena s nikým mimo pracoviště. Stačí pár neopatrných kliknutí a citlivá data na vašem notebooku mohou vystavena na odiv celému světu. V ideálním případě používejte pracovní zařízení pouze k pracovním činnostem a nedovolte, aby je používal někdo jiný.

Vědět, co dělat, když ztratíte pracovní zařízení.

Ztráta pracovního zařízení je nepříjemná, ale všichni víme, že se to čas od času může stát. Kromě toho, že byste měli být na firemní zařízení opatrní (jste za něj zodpovědní), měli byste vědět, co dělat, když taková situace nastane. Neváhejte se obrátit na IT oddělení, aby mohlo problém rychle vyřešit. A i když jste nikdy o žádné pracovní zařízení nepřišli, je lepší být připraven. Zeptejte se svého IT oddělení, co v takových situacích dělat a seznamte se se správným postupem.

Neodkládejte žádné aktualizace.

Používání zastaralé verze aplikace nebo softwaru může představovat zbytečné bezpečnostní riziko. Pokud jste informováni o nově vydané aktualizaci softwaru, zbytečně ji neodkládejte. Pokud vás vyskakovací okno s požadavkem na aktualizaci překvapí, neváhejte se obrátit na IT oddělení. Jako další opatření musí IT specialisté zkontrolovat, zda nejnovější verze zůstávají stejně bezpečné, jako byly verze starší.

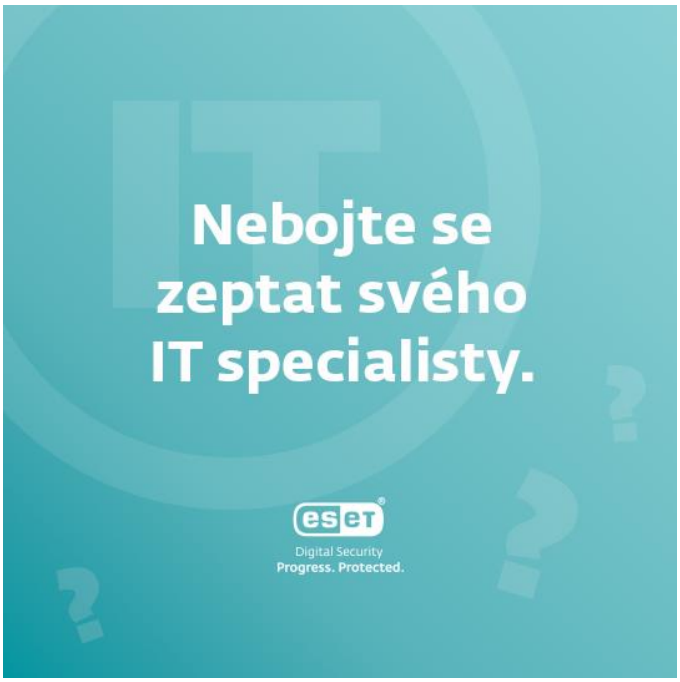


Pro pracovní komunikaci používejte pouze určené kanály.

Pokud jde o pracovní komunikaci, její obsah může sahat od sdílení citlivého dokumentu až po dotaz na kolegu, zda se chce sejít na oběd. V každém případě však existují vhodné kanály, které můžete používat a které byly vybrány na základě úrovně zabezpečení. Používání neschválených aplikací může skončit tím, že se vaše zprávy a dokumenty stanou přístupné lidem mimo vaši práci, což může ohrozit vaši společnost kvůli možného úniku dat. Ujistěte se, že víte, které stránky a aplikace můžete pro komunikaci používat, a pokud si nejste jisti, neváhejte se obrátit na své IT specialisty.

Sdílení odkazů může být riskantní operací.

Potřebujete sdílet citlivý dokument se svým kolegou? Namísto vytváření veřejného odkazu pro sdílení povolte přístup přímo vybraným osobám s ověřenou identitou. Pokud sdílíte něco mimo vaši organizaci, v ideálním případě zvolte časově omezený přístup. Rovněž sdílení materiálů souvisejících s prací na soukromé e-mailové adresy není vhodné. Ptáte se proč? Abyste minimalizovali riziko, že se nějaká informace dostane do nesprávných rukou.



Nebojte se zeptat svého IT specialisty.

Zajímá vás, co dělat, když obdržíte podezřelý e-mail? Nejste si jisti, jak bezpečně sdílet dokument s kolegy? Žádná otázka není hloupá, proto se nebojte zeptat specialistů z vašeho IT oddělení. Nebojte se, že budete plýtvat jejich časem. Vaše zodpovědnost a obezřetnost jim může z dlouhodobého hlediska ušetřit spoustu času a problémů. Vždy je lepší zůstat informovaný a v bezpečí, než čelit nějakým závažnějším problémům a řešit jejich následky.