Příliš snadné placení online: Češi si věří víc, než by měli. Touha po slevách a nákupy z gauče nahrávají podvodníkům

23.4.2026 - | mBank

Češi se v online prostředí cítí velmi sebejistě, ale toto sebevědomí je často falešné. Zatímco většina z nás věří, že ví, jak své peníze chránit, počet obětí kybernetických útoků roste. Nový průzkum výzkumné agentury Focus pro mBank ukazuje, že naše touha po pohodlí a nízkých cenách z nás dělá snadné terče. Podvodníci navíc stále častěji využívají umělou inteligenci a hrají jim do karet základní chyby, jako je ukládání hesel v prohlížeči nebo nákupy přes veřejné Wi-Fi sítě.

Průzkum mBank ukázal výrazný paradox: Každý pátý Čech by si ze znalostí bezpečného chování při online nákupech dal s klidem jedničku. Celých 81 % lidí pak tvrdí, že přesně ví, jak své finance na internetu chránit. Realita je však mnohem varovnější. *„Právě falešné e-shopy jsou dnes druhým nejčastějším typem úspěšného podvodu,“* vysvětluje Robert Chrištof, generální ředitel mBank pro Českou republiku. Podle dat má zkušenost s podvodným e-shopem už každý čtvrtý nakupující (25 %) a zhruba každý sedmý (14 %) už kvůli nim reálně přišel o peníze.

Pohodlí vítězí nad opatrností: Nakupujeme v noci i z toalety
Důvodem, proč lidé tak snadno naletí, je především upřednostňování rychlosti a pohodlí před obezřetností. Bezpečnosti věnujeme čím dál menší pozornost a naše nákupní rituály jsou pro útočníky ideální příležitostí.

- Více než polovina lidí (54 %) nakupuje nejraději z pohodlí gauče.
- Třetina nakupujících (34 %) vyřizuje objednávky večer nebo v noci.
- Často podléháme emocím a slevám v situacích, kdy se nesoustředíme – lidé klidně odkliknou nákup i na toaletě.

„Alarmující je, že pouze 25 % lidí při nákupu řeší, zda daný e-shop vůbec zná,“ upozorňuje Tomáš Mika, expert mBank na kybernetickou bezpečnost. Hlavním lákadlem totiž zůstávají nízké ceny, což je právě ta nejčastější karta, na kterou podvodníci sázejí.
Umělá inteligence a lidský faktor
Kybernetické podvody se neustále vyvíjejí. Ačkoliv se 61 % lidí podvodu vůbec neobává, téměř polovina (48 %) už se někdy stala jeho obětí. Velkým tématem je nyní umělá inteligence, která hraje roli na obou stranách barikády. Pomáhá bankám chránit klienty, ale útočníkům slouží k vytváření propracovaných deep fake videí nebo kopií stránek oblíbeného e-shopu.
Přestože technologie postupují, nejslabším článkem zůstává člověk. *„Manipulace a sociální inženýrství jsou nejsnazší cestou k úspěchu,“* komentuje Tomáš Mika a pokračuje v upozorňování na základní chyby: *„Problémem je například přístup lidí k heslům. Silná hesla sice zná 97 % lidí, ale reálné chování je jiné. Třetina (30 %) si je ukládá do prohlížeče a 40 % lidí běžně nakupuje přes nezabezpečenou veřejnou Wi-Fi.“* Právě to jsou otevřené dveře pro útočníky, kteří se tak mohou k citlivým datům dostat velmi snadno.
„Z dlouhodobého hlediska se potvrzuje, že klíčovou roli nehraje jen technologická gramotnost, ale především lidské rozhodování v konkrétních situacích. Ve chvíli, kdy do hry vstupují emoce, časový tlak nebo rutina, jde racionální uvažování stranou. To je přesně prostor, který dnešní podvodníci velmi efektivně využívají,“ konstatuje Martin Slosiarik, sociolog a ředitel agentury Focus.
Právě klienti samotní drží od pomyslných bezpečnostních dveří klíč. Podvodníci dnes nejčastěji cílí

na emoce – snaží se vyvolat strach nebo časový tlak nebo falešný pocit výhodné nabídky, případně se vydávají za autority. mBank proto dlouhodobě upozorňuje, aby klienti nikdy nesdělovali své přihlašovací údaje, PINy ani autorizační kódy, a to ani osobám, které se vydávají za bankéře či policii. Důležité je také pečlivě kontrolovat odkazy v e-mailech a SMS zprávách, ověřovat si informace z oficiálních zdrojů a reagovat s rozvahou. Pokud „něco nesedí“, je vždy lepší komunikaci ukončit nebo se obrátit přímo na banku.

Jak klientům pomáhá banka? mBank nabízí digitální „štíty“

Pokud už dojde ke krizové situaci, 56 % Čechů by jako první kontaktovalo svou banku. Právě banky hrají klíčovou roli v edukaci a prevenci v oblasti kyberbezpečnosti. *„Zatímco 80 % Čechů se dnes spoléhá na nastavení limitů na svých kartách, my v mBank jdeme ještě dál a nabízíme řešení, která útokům aktivně předcházejí,“* vysvětluje Martin Podolák, ředitel produktů a inovací mBank, a dodává: *„Patří mezi ně například ověření volajícího nebo e-mailu přímo v mobilní aplikaci, které funguje podobně jako ikonka ověřeného profilu na sociálních sítích. Klient tak hned vidí, že mluví skutečně s bankou. Pro bezpečné online nákupy pak nabízíme už od roku 2021 dobíjecí eKartu, kterou lze využít jako digitální štít oddělený od hlavního účtu.“* Tuto kartu měsíčně využívá 29 tisíc lidí, a to zejména pro nákupy na zahraničních e-shopech, kde je její podíl na transakcích mimo EU o 46 % vyšší než u běžných karet.

„I přes moderní zabezpečení systémů bank zůstává nejdůležitější složkou bezpečnosti sám uživatel. Zdravá nedůvěra k podezřele nízkým cenám a pečlivost při nakládání s hesly jsou i v době umělé inteligence tou nejlepší ochranou,“ dodává Tomáš Mika.

Silná hesla jsou jedním ze základů bezpečného chování v online světě. Další opatření, kterými se lidé mohou na internetu chránit, připomíná bezpečnostní desatero mBank, které banka uvádí na svém webu www.mbank.cz/bezpecnost.

Reprezentativní kvantitativní průzkum mezi online populací ČR ve věku od 18 do 60 let mBank realizovala ve spolupráci s agenturou Focus v lednu 2026. Zúčastnilo se ho 1 018 respondentů. Data byla sbírána formou online dotazníku.

https://cz.media.mbank.pl/455474-prilis-snadne-placeni-online-cesi-si-veri-vic-nez-by-meli-touha-po-slevach-a-nakupy-z-gauce-nahravaji-podvodnikum