

Průzkum ESET: Nejvíce si v Česku píšeme přes WhatsApp, zabezpečení ale věnujeme okrajovou pozornost

17.3.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

Nejoblíbenější komunikační platformou v Česku je WhatsApp. Vyplývá to z nejnovějšího průzkumu společnosti ESET připraveném v aplikaci Instant Research od agentury Ipsos. Mezi další nejoblíbenější komunikační nástroje patří také Facebook Messenger, Instagram, iMessage či Telegram. Třetina dotázaných považuje AI rozšíření v komunikačních platformách za užitečné, přesto tyto nástroje většina z nás zatím nepoužívá. Skoro polovina uživatelů a uživatelky v Česku se již na komunikačních platformách setkala s kybernetickým podvodem. Když ale přijde řada na bezpečnost, orientujeme se především ve dvoufaktorové autentizaci a zálohování konverzací. Ostatní bezpečnostní prvky zatím příliš nevyužíváme.

Nejoblíbenější komunikační platformou v Česku je WhatsApp – využívá ji 89 % Čechů a Češek. Jako alternativu k ní dále nejvíce volíme Facebook Messenger (78 %). V čele žebříčku nepoužívanějších aplikací ke komunikaci se pak objevila také platforma Instagram (31 %) či aplikace iMessage určená pro uživatele zařízení s platformou iOS od společnosti Apple (13 %). Desetina dotázaných také potvrdila, že využívá platformu Telegram (11 %).

„Není velkým překvapením, že lidé v Česku volí ke komunikaci nejvíce WhatsApp. Úplně nejoblíbenější je podle výsledků v Praze, na Moravě zase vede právě Facebook Messenger. Aplikace WhatsApp dlouhodobě vychází jako jedna z těch bezpečnějších variant pro komunikaci, i díky silnému šifrování a nabídce bezpečnostních nástrojů, které nadále rozšiřuje. Letos v lednu například společnost Meta představila nové ‚přísné nastavení účtu‘, které po zapnutí automaticky blokuje média a přílohy od neznámých odesílatelů, ztiší hovory z neznámých čísel, vypne náhledy odkazů a aktivuje omezení pro zprávy od neznámých kontaktů. Právě kybernetické podvody, které nezřídka míří i přímo na české uživatele a uživatelky, jsou naopak něčím, co tuto platformu dlouhodobě sužuje a v kontrastu s její oblibou představuje riziko,“ říká Ondřej Novotný, kyberbezpečnostní analytik v pražské výzkumné pobočce společnosti ESET.

Zajímavé rozdíly ukázal průzkum dále u platforem Discord či Snapchat, a to u jednotlivých věkových skupin respondentů. Zatímco lidé ve věku 31 let a starší používají tyto platformy jen okrajově, neplatí to pro nejmladší uživatele a uživatelky. Discord jako nástroj ke komunikaci využívá pětina (21 %) lidí ve věku 18–30 let, zatímco Snapchat využívá téměř čtvrtina lidí z této věkové skupiny (24 %).

„Jak můžeme vidět na základě výsledků, na jedné straně máme komunikační platformy, které fungují více jako klasický ‚telefonní‘ adresář. Lidi, se kterými komunikujeme, v převážné většině případů nějak známe, a pokud nás kontaktuje někdo cizí, platforma ho označí. Typicky takhle fungují právě WhatsApp nebo Facebook Messenger. Na druhé straně tu ale máme Discord a Snapchat, což jsou platformy, které jsou daleko více otevřené komunikaci s neznámými lidmi. Více připomínají sociální síť a z toho pro ně například plynou větší rizika útoku pomocí [technik sociálního inženýrství](#), typicky phishingu,“ vysvětluje Novotný.

Zdrojem podvodných zpráv s nebezpečnými odkazy mohou být i tzv. kanály, ať už pro komunikaci v rámci komunit, či v podobě odběru novinek různých tematických profilů přímo v komunikační platformě. Nějaký typ kanálu sleduje již nyní více než čtvrtina dotázaných (29 %) lidí v Česku. Jedná

se především o lidi ve věku 18 až 30 let. Naopak dvě pětiny (41 %) lidí uvedly, že odběr kanálů nevyužívají a ani to neplánují.

AI v chatech považujeme za užitečnou, přesto ji nepoužíváme

Nejednoznačný názor mají Češi také na AI rozšíření, které dnes řada komunikačních platforem nabízí. Uživatelé díky [umělé inteligenci](#) mohou například vyhledávat informace, překládat texty, upravovat videa a fotky či shrnout dlouhé konverzace a vlákna. Rozšíření v podobě nástrojů umělé inteligence ale většina uživatelů (60 %) nevyužívá. Umělou inteligenci naopak zapojí dle průzkumu pětina lidí (19 %).

„V otázce využívání nástrojů umělé inteligence jsme zaznamenali poměrně značnou nesourodost v odpovědích. Využívání AI v komunikačních aplikacích potvrzovali především lidé se základním vzděláním a s výučním listem, jednalo se také o lidi v nejmladší věkové kategorii 18–30 let a o něco více takto odpovídaly ženy. Desetina dotázaných pak netuší, zda komunikační platforma, kterou využívají, takové rozšíření má. Na druhou stranu pak v otázce, zda AI v komunikačních platformách považují lidé za užitečnou, odpovídali kladně nejvíce lidé ve věku 41–50 let a 51–65 let. Jednalo se celkově o 31 % dotázaných. Za neužitečné rozšíření to považuje 24 % dotázaných a více než třetina lidí uvedla, že by si to ještě potřebovali vyzkoušet,“ shrnuje výsledky Novotný.

„Jasně je zde vidět, že uživatelé a uživatelky v Česku ještě asi nemají na využívání nástrojů umělé inteligence ustálený názor. O to větší obezřetnost je ale podle mě na místě. Pokud nějaký nástroj nebo technologii neznáme, nebo ji známe pouze povrchně, právě nedostatek znalostí a informací může hrát do karet kyberútočníkům. Pokud nevíme, co AI nástroje v nějaké aplikaci dokážou, můžeme se stát snadněji obětí například deepfake obsahu vytvořeného právě umělou inteligencí. Více než kdy dřív je tak důležité z mého pohledu plošné vzdělávání v nástrahách dnešního online světa,“ dodává Novotný.

Komunikační platformy jsou dějištěm kyberpodvodů

Hlavním důvodem, proč některou komunikační platformu používáme, je dle průzkumu naše rodina a přátelé, kteří danou aplikaci využívají také. Jak se ale zajímáme o skutečné bezpečnostní prvky, které lze v rámci komunikačních platforem nastavit, a posílit tak zabezpečení svých dat?

„V průzkumu nás zajímalo, jak uživatelé a uživatelky v Česku využívají v rámci komunikačních platforem tzv. [dvoufaktorovou autentizaci](#). Jedná se o potvrzení přístupu nebo nějaké operace dalším prvkem nad rámec klasického hesla a zpravidla jde o kód zaslaný do SMS zprávy, autentizační aplikace nebo potvrzení biometrickými údaji – skenem otisku prstu nebo obličeje. Čtvrtina dotázaných uvedla, že dvoufaktorovou autentizaci využívá jen u těch aplikací, které používá nejčastěji, další necelá čtvrtina pak toto dodatečné zabezpečení využívá všude, kde je to možné. Zdá se, že tento způsob ochrany dat je již v naší společnosti dobře adaptovaný. Přesto jej za zbytečný považuje pětina dotázaných,“ doplňuje Novotný.

Komunikační platformy nabízejí ještě další nástroje, jak posílit bezpečnost svého účtu a dat v online komunikaci s dalšími lidmi. Třetina uživatelů a užívatelky je však vůbec nevyužívá. Ti, kteří hledají větší zabezpečení, pak nejvíce využívají zabezpečené zálohování konverzací (26 %). Pětina lidí (21 %) dále skrývá svou polohu, 13 % využívá funkci pouze jednoho zobrazení fotky či videa a desetina dotázaných využívá jak ztišení hovorů od neznámých volajících, tak tzv. mizející zprávy.

„S kybernetickým podvodem na komunikačních platformách se podle průzkumu setkala již skoro polovina Čechů a Češek. Zatímco většina z nich uvedla, že podvod včas rozpoznala a žádná škoda jim

nevznikla, v desetině případů buď přišli o svůj účet nebo o peníze. Právě v případě platformy WhatsApp se již od minulého roku objevuje například [falešná výzva k hlasování v soutěži](#), o které vás žádá útočník prostřednictvím odcizeného účtu vašich přátel, nebo dokonce příbuzných. To, že se tento útok opakovaně objevuje, jen svědčí tom, že je do jisté míry stále úspěšný," říká Novotný. „Pokud zůstaneme u platformy WhatsApp jako nejpoužívanější chatovací aplikace, rozhodně platí, aby uživatelé nikdy nikam nepřeposílali ověřovací kódy této aplikace. Také bychom opět neměli klikat na odkazy a stahovat dokumenty od neznámých lidí, nebo od kontaktů, se kterými komunikujeme jen sporadicky a najednou se ozvou s nějakým požadavkem. Vždy je na místě si takovou zprávu ověřit. Samozřejmostí je také zapnuté vícefázové ověření a pravidelná kontrola ostatních připojených zařízení v rámci našeho účtu. V neposlední řadě je také důležité aplikace i systém chytrého telefonu pravidelně aktualizovat," doplňuje Novotný z ESETu.

Spolehlivou ochranou i pro komunikační platformy je [moderní bezpečnostní software](#), který na svém chytrém telefonu využívá polovina (50 %) dotazovaných. Ten dokáže rozpoznat kromě závažných škodlivých kódů také odkazy na nebezpečné phishingové stránky. Čtvrtina dotázaných (26 %) stále takový program nevyužívá a desetina netuší (13 %), zda ho využívá či nikoli.

Sběr dat byl realizován prostřednictvím aplikace Instant Research agentury Ipsos ve dnech od 4. do 6. března 2026 na 1052 respondentech v České republice.

O společnosti ESET

Společnost ESET®, která byla založena v Evropě, je předním dodavatelem řešení kybernetické bezpečnosti s pobočkami po celém světě. Poskytuje špičková řešení kybernetické bezpečnosti, která pomáhají předcházet útokům ještě před jejich vznikem. ESET kombinuje technologie umělé inteligence (AI) a lidskou odbornost, čímž pomáhá předejít nově vznikajícím globálním kybernetickým hrozbám, ať již známým či dosud neznámým. Poskytuje zabezpečení pro firmy, kritickou infrastrukturu a jednotlivce. Ať už jde o ochranu koncových zařízení, cloudu nebo mobilních zařízení, řešení a služby společnosti ESET, které využívají technologie umělé inteligence a kladou důraz na cloudové prostředí, zůstávají vysoce efektivní s minimálními nároky na uživatele.

Technologie ESET jsou vyvíjeny v EU a zahrnují robustní systém detekce a reakce, ultra-bezpečné šifrování a multifaktorovou autentizaci. S nepřetržitou obranou v reálném čase a silnou místní podporou udržuje ESET uživatele v bezpečí a firmy v chodu bez narušení jejich provozu. Neustále se vyvíjející digitální prostředí vyžaduje progresivní přístup k bezpečnosti. Jen v České republice nalezneme tři výzkumná a vývojová centra společnosti, a to v Praze, Jablonci nad Nisou a Brně. Výzkumné pobočky po celém světě podporují aktivity společnosti v rámci Threat Intelligence, stejně jako její silná globální síť partnerů.

Více informací

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost naleznete například v online magazínu [Dvojklik.cz](#) nebo v online magazínu o IT bezpečnosti pro firmy [Digital Security Guide](#). Nejčastějším rizikům pro děti na internetu se věnuje iniciativa [Safer Kids Online](#), která má za cíl pomoci nejen jejich rodičům, ale také například učitelům či vychovatelům zorientovat se v nástrahách digitálního světa.

Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách [Slovníku ESET](#), v [podcastu RESET](#) a na našich sociálních sítích [Facebook](#), [Instagram](#), [LinkedIn](#) a [X](#).

Lucie Mudráková
Specialistka PR a komunikace

ESET software spol. s r.o.
tel: +420 702 206 705
lucie.mudrakova@eset.com

Vítězslav Pelc
Senior manažer PR a komunikace
ESET software spol. s r.o.
tel: +420 720 829 561
vitezslav.pelc@eset.com

<https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/pruzkum-eset-nejvice-si-v-cesku-piseme-p-res-whatsapp-zabezpeceni-ale-venuujeme-okrajovou-pozornost>