Tři hlavní digitální hrozby, které vážně ohrožují soukromí i vztahy

3.10.2024 - | PROTEXT

Globální společnost Kaspersky, která se zabývá kybernetickou bezpečností a digitálním soukromím, upozorňuje v rámci Evropského měsíce kybernetické bezpečnosti na rostoucí rizika, která moderní technologie představují pro společenské vztahy.

Na základě vlastního nezávislého výzkumu identifikovala společnost Kaspersky tři klíčové hrozby, které se v důsledku technologického pokroku ještě více prohloubily.

1. Zneužívání intimních snímků: když se soukromé snímky vymknou kontrole

Průzkum, kterého se v květnu 2024 zúčastnilo 9 033 lidí po celém světě, ukázal, že čtvrtina (25 %) respondentů sdílela soukromé snímky s osobami, s nimiž se seznámili online, přičemž mezi lidmi ve věku 25–34 let tento podíl vzrostl na 39 %. K tomu jednání jsou obzvláště náchylní muži – 20 % z nich přiznává, že posílá intimní snímky lidem, které osobně nikdy nepotkali. Tato forma digitální důvěry je snadno zneužitelná a může vést k tzv. „pornografii z pomsty“ (revenge porn). Zejména mezi mladšími generacemi uvádí zkušenosti s touto formou zneužíváním na internetu 69 % osob ve věku 16–24 let, což odhaluje zásadní společenský problém.

2. Stalkerware: když dochází ke zneužití legitimní technologie

Stalkerware – sledovací aplikace maskované jako legitimní nástroje – se stává stále větším problémem. Údaje společnosti Kaspersky ukazují, že v letech 2022 až 2023 došlo k 5,8% nárůstu těchto případů, které zasáhly do života více než 31 000 osob po celém světě. V Evropě patřily v roce 2023 k nejvíce postiženým zemím Německo, Francie a Spojené království. Stalkerware je však často jen jedním z aspektů širšího modelu zneužívání. V dnešním vysoce propojeném světě mohou pronásledovatelé využívat ke sledování svých obětí sociální média, chytrá domácí zařízení a GPS i bez nutnosti instalovat stalkerware.

3. Deepfakes: když se padělky stávají nerozeznatelnými od reality

Nebezpečným nástrojem v osobních vztazích se stává technologie deepfake, která umožňuje vytvářet pomocí umělé inteligence realistické obrázky, videa nebo zvukové záznamy. Tato technologie se v posledních pěti letech rychle rozvíjela a nyní jsou volně k dispozici různé nástroje s otevřeným zdrojovým kódem, které umožňují vytvářet „fejkovou realitu“ každému, kdo má základní programátorské dovednosti. V důsledku toho se deepfakes mohou stát jedním z nejnebezpečnějších nástrojů budoucnosti s rostoucím potenciálem pro vytváření falešného kompromitujícího obsahu, který by mohl být použit k vydírání a nátlaku ve vztazích.

Tyto problémy zdůrazňují rostoucí potřebu digitální gramotnosti a online bezpečnosti v dnešním technologiemi ovládaném světě. **David Emm**, hlavní bezpečnostní výzkumník z týmu Kaspersky Global Research and Analysis Team, radí: *„Řešení těchto moderních forem zneužívání ve vztazích vyžaduje mnohostranný přístup. Za prvé je třeba vysvětlovat koncept ‚trvalého souhlasu‘. Za druhé se ukazuje jako nezbytné cílené vzdělávání celé společnosti, protože obviňování obětí je stále výrazným problémem, který jen prohlubuje jejich trauma a odvádí pozornost od odpovědnosti pachatelů. A konečně, zásadní význam pro to, aby byli lidé schopni chránit své soukromí a účinně zvládat příslušná rizika, má zvyšování digitální gramotnosti. Uplatněním těchto strategií můžeme*

vybudovat kulturu respektu, odpovědnosti a informované ochrany před zneužíváním.“

Společnost Kaspersky se zabývá kybernetickou bezpečností a poskytuje ochranu proti široké škále digitálních hrozeb. Některá nebezpečí, jako je grooming a doxing, stalking, šikana nebo zneužití intimních snímků, však přesahují možnosti samotné technologie. Proto je zásadní osvěta veřejnosti a společnost Kaspersky se jako specializovaná organizace snaží zvyšovat povědomí o těchto hrozbách a umožnit lidem, aby se dokázali chránit sami.

Chcete-li se o těchto hrozbách a ochranných opatřeních dozvědět více, navštivte náš blogpost, který obsahuje tuto zprávu, brožuru o nebezpečích digitálního seznamování a online prezentaci Davida Emma.

ČTK Connect ke zprávě vydává obrazovou přílohu, která je k dispozici na adrese https://www.protext.cz.

https://www.ceskenoviny.cz/tiskove/zpravy/tri-hlavni-digitalni-hrozby-ktere-vazne-ohrozuji-soukromi-i-vztahy/2577786