



CRIF CYBER OBSERVATORY

1. pololetí 2023



Kybernetická observatoř CRIF analyzuje zranitelnost lidí a firem vůči kybernetickým hrozbám útokům, interpretuje hlavní trendy týkající se kybernetické výměny dat na webu a předkládá návrhy na zmírnění kybernetických rizik.

OPEN WEB

Indexováno vyhledávači. Přístupné pro všem prostřednictvím nejoblíbenějších prohlížečů prohlížečů.



STUDIE, KTERÁ JDE DO HLOUBKY A ZKOUMÁ PROSTŘEDÍ OPEN WEBU I DARK WEBU.

DARK WEB

Skryté, neindexované vyhledávači. Přístupné prostřednictvím šifrovaného navigačního softwaru, který zaručuje anonymitu.

IDEÁLNÍ MÍSTO PRO HACKERY A KYBERZLOČINCE.



ZÁZNAM OSOBNÍCH ÚDAJŮ, KTERÉ KOLUJÍ NA DARK WEBU.

VÍCE NEŽ 950 000 CRIF KYBERNETICKÝCH VÝSTRAH



Alerty

o kybernetických útocích
na osobní údaje uživatelů.



Odcizené informace mohou být použity k různým účelům, například k **prolomení účtů** obětí, zneužití služeb a **vydírání** nebo krádeži peněz. Často jsou použity k podvodům, jako je **phishing** nebo **smishing**.



79,5 %

údaje nalezené
na DARK webu

DARK WEB



20,5 %

údaje nalezené
na OPEN webu

OPEN WEB

Nejzranitelnější data na webu



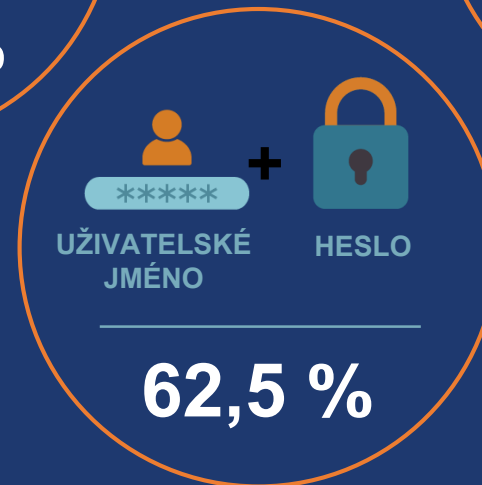
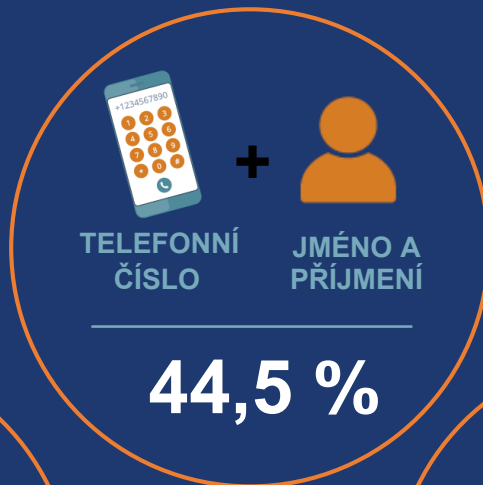
Nejpoužívanější

- 01 123456
- 02 123456789
- 03 heslo



Potvrzuje se, že **hesla a e-maily** jsou spolu s **telefonními čísly nejzranitelnějšími údaji** a jsou cennými údaji pro přístup k mnoha platformám a aplikacím, ve kterých se pracuje s **dvoufaktorovým ověřováním**.

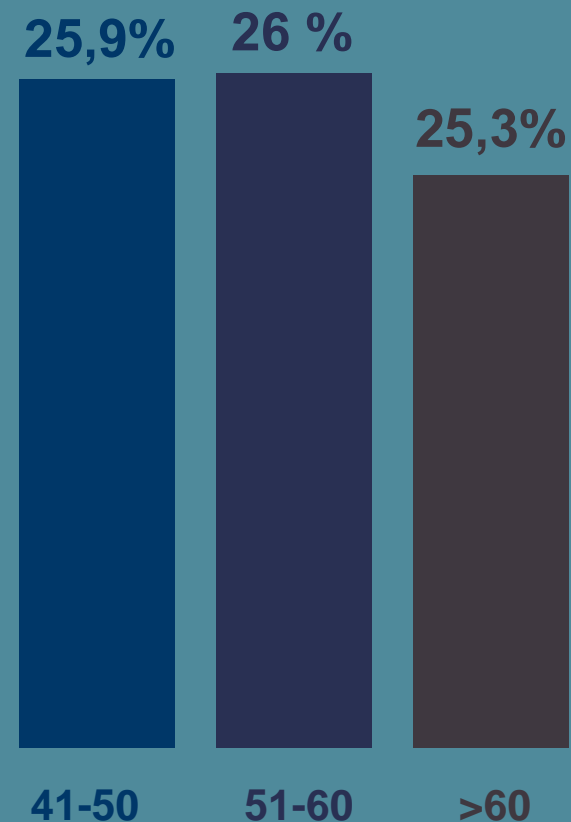
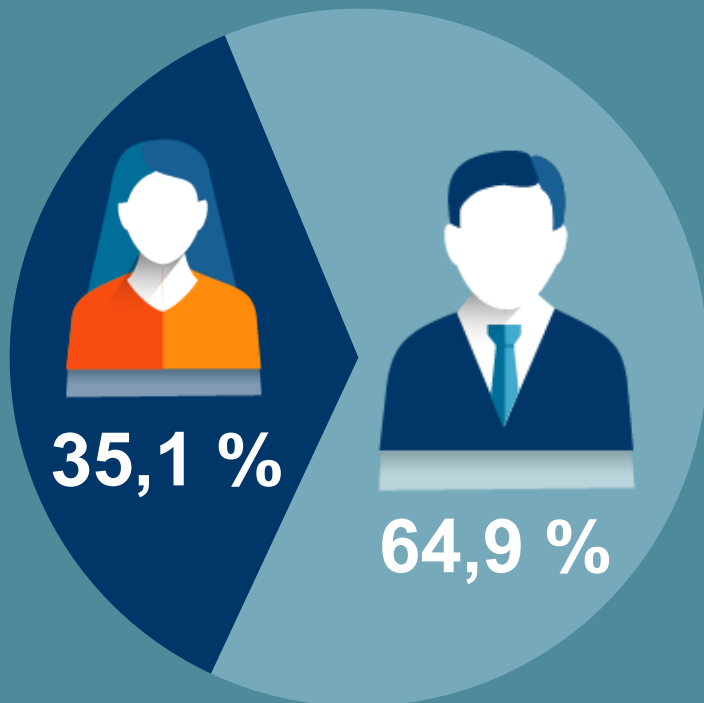
Nejčastější kombinace zachycených dat



Nárůst počtu případů kombinace telefonních čísel a hesel o 372 % oproti předchozímu roku vyvolává stále větší obavy. Hackeři mohou zneužívat telefonní čísla k podvodům, jako jsou podvody založené na SMS (Smishing) nebo výměna SIM karet.

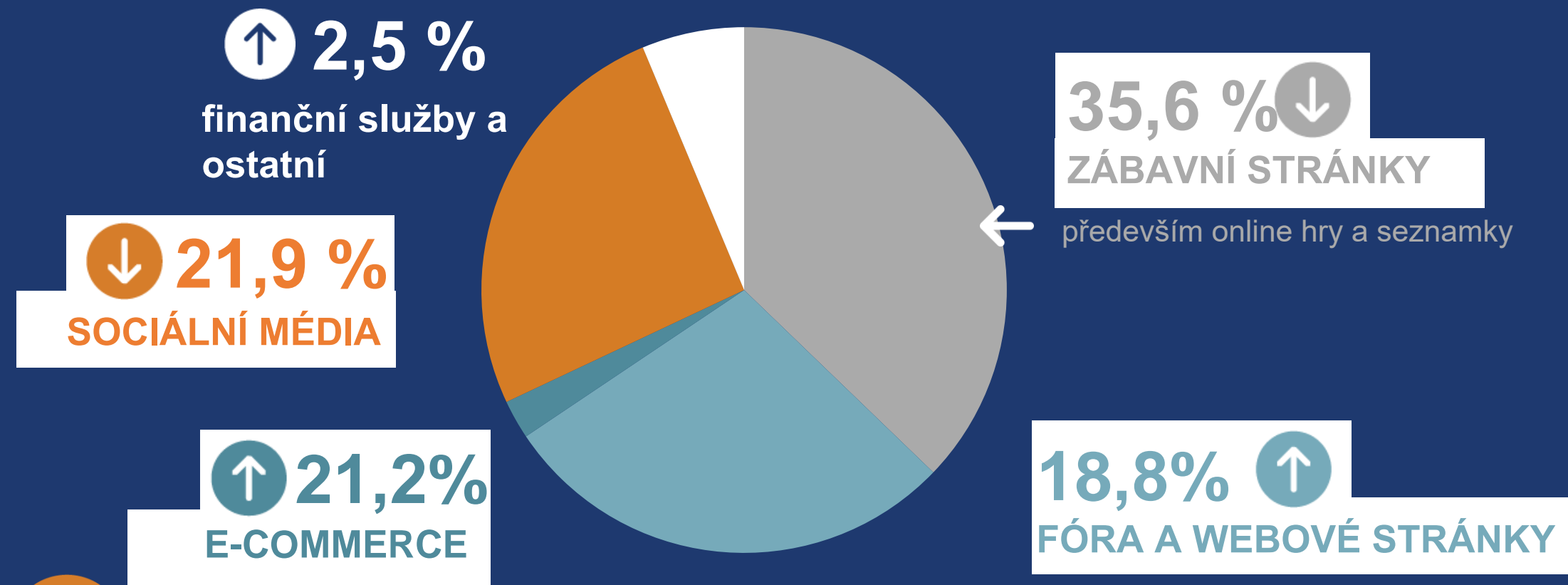
* změna v prvním pololetí 2023 oproti prvnímu pololetí 2022

Profil nejčastěji zasažených uživatelů



Nejvíce postiženými věkovými skupinami jsou **muži nad 40 let**. Mladší generace (ve věku do 30 let) je ohrožena méně, pravděpodobně díky tomu, že lépe zná digitální prostředí.

Nejčastěji kradené typy účtů



Nejčastěji se kradou účty na **zábavních webech**, zejména účty pro online hry a seznamky. **nejvýznamnější nárůst se týká krádeží účtů v elektronických obchodech**, které mohou mít pro oběti přímé ekonomické důsledky.

Nejnovější vydání studie CRIF Cyber Observatory potvrzuje význam našich osobních dat pro podvodníky.

Zejména kontaktní údaje a přihlašovací údaje k účtům jsou pro podvodníky stále atraktivnější, což umožňuje podvody a krádeže identity. Pokud se totiž zločincům podaří získat více osobních údajů, které pomáhají doplnit profil oběti, mohou lépe plánovat útoky, a to i s využitím technik sociálního inženýrství.

Další rostoucí hrozbou je ransomware, zejména proti firmám. Je třeba věnovat zvláštní pozornost e-mailům a zprávám, které denně dostáváme, a trénovat se v rozpoznávání podvodů a pokusů o phishing.



BEZPEČNÉ PROHLÍŽENÍ

Tipy na ochranu před krádeží identity a digitálními podvody



Zvolte si bezpečná hesla

Je důležité zvolit si dlouhá a odlišná hesla pro každý účet, zároveň nepoužívat kombinace související s osobními údaji.



Antivirový software a pravidelná aktualizace

Stále vylepšujte zabezpečení vašich zařízení je nutné je aktualizovat a chránit.



Zálohování dat

Provádějte pravidelné zálohování, abyste zabránili ztrátě dat. Kromě toho si vytvořte kopie dokumentů, abyste je mohli kdykoli obnovit prostřednictvím internetu.



Chraňte svá zařízení

Nastavte zámek obrazovky pomocí kódu PIN, hesla, otisku prstu nebo rozpoznání obličeje a zapněte dálkové ovládání pro vzdálené zamykání. Zabraňte ostatním v jejich používání bez vašeho souhlasu. Nastavte monitorování.



Pozor na podezřelé zprávy, emaily a telefonáty

Vždy se mějte na pozoru před jakýmkoli pokusem o kontakt, který vyžaduje poskytnutí osobních nebo finančních údajů.



Využívání monitorovacích služeb

Nejlepší strategií pro komplexnější ochranu je výběr specifických řešení pro sledování oběhu vašich dat na webu.

Pro více informací:
helpdesk@kolikmam.cz