eset | bezpečne na nete

Aké sú najčastejšie formy útokov cez prehliadač?

- Škodlivé rozšírenia prehliadača
- Útočník v prehliadači
- Drive-by download útok
- Malvér ťažiaci kryptomeny
- Sociálne inžinierstvo
- Scareware
- Škodlivý obsah
- Clickjacking
- Cursorjacking

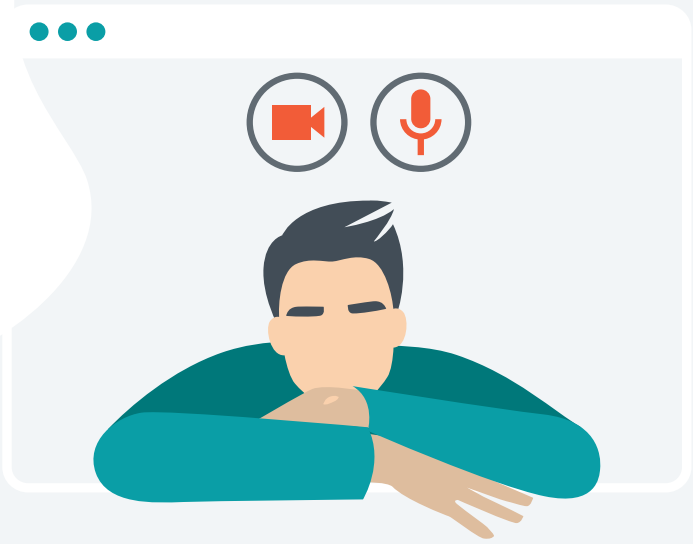
Vysvetlenia hrozieb nájdete na Bezpečne na nete.

Ako môžete zvýšiť bezpečnosť prehliadača?

1. Zapnite v nastaveniach možnosť Safe Browsing, ktorú majú zabudovanú viaceré prehliadače.
2. Zablokujte automatické otváranie okien prehliadača.
3. Surfujte po internete inkognito. Nezabúdajte, že ide len o čiastočné obmedzenie zberu informácií prehliadačom priamo na vašom zariadení.
4. Pravidelne aktualizujte váš operačný systém, prehliadač a pluginy.
5. Zvoľte možnosť automatického odstraňovania súborov cookie.
6. Môžete využiť pripojenie cez Virtual Private Network (VPN), ktoré dokáže vytvoriť šifrovaný tunel medzi zariadením používateľa a cieľovou stránkou.
7. Zabezpečte všetky vaše zariadenia spoľahlivým bezpečnostným softvérom.

eset | bezpečne na nete

Ako rozpoznať (ne)bezpečnú stránku?



- ✓ V URL adrese chýba „s“, čo znamená secure. URL adresa sa začína na http.
- ✓ Chýba kontaktný formulár alebo iný kontakt na prevádzkovateľa webu.
- ✓ Na stránke je množstvo gramatických chýb.
- ✓ Obsah stránky obsahuje lákavé ponuky alebo veľa blikajúcich okien a reklám.

Čo robiť, ak sa dostanem na nebezpečnú webovú stránku?

1. Neklikajte na žiadne prvky, ako sú tlačidlá, obrázky, videá alebo odkazy.
2. V žiadnom prípade z takejto stránky nesťahujte súbory, hudbu či najnovšiu epizódu seriálu.
3. Stránku by ste mali čo najskôr opustiť.
4. Pre vyššiu bezpečnosť odporúčame zariadenie preskenovať bezpečnostným softvérom.
5. Odporúčame aktivovať dvojfaktorové overenie všade tam, kde je to možné.