CERT.hr
surfaj sigurnije

Savjeti Nacionalnog CERT-a za zaštitu u slučaju curenja podataka

U nastavku se nalazi nekoliko savjeta za zaštitu i prepoznavanje prijetnji s kojima se korisnici mogu susresti nakon curenja podataka.
Kriminalci često koriste osobne i kontaktne podatke kako bi njihove prijevare izgledale vjerodostojno. Napadači mogu:

- Slati phishing poruke e-mailom koje izgledaju kao da dolaze od naše organizacije, financijskih institucija, državnih tijela ili drugih pouzdanih pružatelja usluga.
- Upućivati telefonske pozive ili slati poruke predstavljajući se kao korisnička podrška, sigurnosni timovi, prijatelji ili netko drugi.
- Koristiti osobne podatke kako bi stekli vaše povjerenje i naveli vas da otkrijete lozinke, financijske podatke ili druge osjetljive informacije.
- Pokušati preuzeti vaše korisničke račune koristeći javno dostupne informacije.
- Počiniti prijevare povezane s krađom identiteta.

Kako prepoznati moguću prijevaru

Budite posebno oprezni prema neočekivanim porukama i pozivima, osobito ako:

- Stvaraju osjećaj straha ili hitnosti te vas prisiljavaju da odmah poduzmete određene radnje (npr. uplatite novac, promijenite lozinku i sl.).
- Traže lozinke, jednokratne autentifikacijske kodove ili financijske podatke.
- Traže da kliknete na poveznice, otvorite privitke ili instalirate softver.
- Tvrde da će vaš račun biti blokiran ili ukinut ako odmah ne reagirate.
- Sadrže neuobičajene adrese pošiljatelja, pravopisne pogreške ili sumnjive poveznice.
- Zahtijevaju nastavak komunikacije putem drugog kanala. Prevaranti često traže da nastavite razgovor putem WhatsAppa ili nekog drugog servisa kako bi izbjegli otkrivanje.

Što možete učiniti kako biste se zaštitili

Preporučujemo da poduzmete sljedeće mjere:

- Promijenite lozinke u kojima koristite osobne podatke kao dio lozinke ili sigurnosnih pitanja. Savjete za dobru lozinku možete pronaći ovdje.
- Uključite višefaktorsku autentifikaciju (MFA/2FA) gdje god je dostupna. Time se značajno povećava sigurnost računa čak i ako lozinka bude kompromitirana.
- Redovito pratite svoje korisničke račune, elektroničku poštu i druge komunikacije radi otkrivanja sumnjivih aktivnosti.
- Budite oprezni pri odgovaranju na neočekivane poruke i pozive, čak i ako pošiljatelj raspolaže nekim vašim osobnim podacima.
- Sumnjive zahtjeve provjerite drugim kanalom komunikacije. Npr. ako vas netko nazove i uvjerava da je vaše dijete ili prijatelj u opasnosti, provjerite tu informaciju tako da ih sami nazovete ili im pošaljete osobno poruku.

Podsjećamo da vas nikada nećemo tražiti da putem e-maila, SMS-a ili telefonskog poziva otkrijete svoju lozinku, kodove za višefaktorsku autentifikaciju ili druge osjetljive podatke za pristup računima. CARNET s korisnicima komunicira putem službene e-mail adrese helpdesk@carnet.hr.