Projekat finansira Evropska unija

e-business DEVELOPMENT

Република Србија
Министарство трговине, туризма и телекомуникација

Република Србија
Министарство привреде

OSNOVE BEZBEDNOSTI NA INTERNETU

ŠTA JE VISOKOTEHNOLOŠKI KRIMINAL, E-KRIMINAL ILI SAJBER KRIMINAL?

Visokotehnološki kriminal, poznat i kao e-kriminal ili sajber kriminal, obuhvata skup krivičnih dela koja podrazumevaju upotrebu interneta, računara ili nekih drugih elektronskih uređaja. Pojedini oblici e-kriminala direktno su vezani za računare, kao što su širenje opasnih elektronskih virusa koji onesposobljavaju računarski sistem tako da on odbija da izvrši bilo koju uslugu ovlašćenog korisnika. Ostali oblici e-kriminala obuhvataju prevare, govor mržnje, krivična dela protiv intelektualne svojine, kao i proizvodnju, posedovanje i distribuciju spornog materijala.

ŠTA JE KRAĐA IDENTITETA?

Krađa identiteta se događa kada neko prisvoji identitet druge osobe, kao što su ime, detalji o bankovnom računu ili broj kreditne kartice, da bi počinio prevaru ili druga krivična dela. Krađa identiteta je jedna od kriminalnih aktivnosti koja ima najbrži rast na svetskom nivou i ne poznaje geografske granice – žrtve i prestupnici mogu biti na suprotnim stranama sveta. Najveći broj krivičnih dela krađe identiteta počini se uz pomoć računara i drugih elektronskih uređaja. Može da obuhvati krađu

- brojeva platnih i kreditnih kartica,
- pasoša,
- imena,
- adrese,
- podataka iz vozačke dozvole,
- podataka za prijavljivanje za ostale usluge.

KAKO DA SE ZAŠTITITE OD KRAĐE IDENTITETA?

- Nemojte da dajete svoje lične podatke preko telefona, lično ili preko računara, ukoliko niste sigurni da je reč o proverenoj osobi ili organizaciji.
- Nikada ne zapisujte PIN brojeve za svoje platne ili kreditne kartice na samim karticama ili bilo kom dokumentu ili papiru u novčaniku.
- **N**a bezbedan način se rešite ličnih podataka (iscepajte papire, obrišite/uklonite hard diskove iz računara pre prodaje ili bacanja).
- Količinu dokumenata koju svakodnevno nosite sa sobom ili ostavljate u kolima svedite na minimum.
- **Proverite** da li na izvodima iz banke i izvodima o stanju na kreditnoj kartici ima neodobrenih transakcija. Odmah prijavite bilo kakva neslaganja ili neovlašćene aktivnosti banci ili izdavaocu kartice.
  Budite naročito oprezni kada ostavljate lične podatke na javno dostupnim vebsajtovima. Lični podaci mogu biti zloupotrebljeni na više načina od strane kradljivaca identiteta koji pretražuju vebsajtove.

e-business DEVELOPMENT

ŠTA JE TO *MALWARE* ILI ZLONAMERNI SOFTVER?

Malware ili zlonamerni kod predstavlja pretnju po računare i njihovu bezbednost koju ugrožavaju računarski špijuni (engl. spyware), virusi, računarski crvi, trojanci i botovi. To su veoma rasprostranjeni programi koji mogu da evidentiraju sve što ukucate na računaru, da naprave snimke ekrana, ukradu dokumenta i datoteke i otvore skrivena zadnja vrata do vašeg računara. Ove informacije se zatim šalju osobi **koja** je instalirala neki od navedenih programa.

Malware može da instalira svako ko ima pristup računaru ili može biti skriven u „bezopasnom" prilogu poslatom putem e-pošte ili otpremljen putem sumnjivog vebsajta.

KAKO DA SE ZAŠTITITE OD ZLONAMERNIH SOFTVERA?

Ne možete uvek da znate da li imate neki zlonamerni softver u svom računaru, tako da je važno da imate najnoviju verziju softvera koji detektuje viruse instaliranu u vašem računaru. Proverite da li vas taj softver štiti i od računarskog špijuna. Možete da uradite i sledeće:

- Budite svesni toga da kada god koristite računar na javnom mestu poput internet kafea ili biblioteke, on može da sadrži zlonamerni softver napravljen u svrhu prikupljanja vaših podataka.
- Ažurirajte svoj operativni sistem.
- **Budite** pažljivi sa programima za razmenu datoteka – ukoliko nisu pravilno konfigurisani, ostali mogu imati pristup svim vašim datotekama.
- Povećajte nivo zaštite na vašem pretraživaču tako da ne prihvatate cookies sa neproverenih vebsajtova.
- Nikad nemojte da kliknete na link u e-pošti jer vas možda neće odvesti na dati vebsajt.
- **Budite** pažljivi kada otvarate priloge, jer oni mogu da zaraze vaš računar.
- Budite pažljivi kada preuzimate programe sa interneta, koristite proverene izvore i preuzete materijale skenirajte na viruse.
- Budite oprezni sa vebsajtovima koje koriste iskačuće forme (engl. *pop-ups)* ili deluju sumnjivo, jer mogu biti opasni.
- **Koristite** jedinstvenu lozinku za internet bankarstvo koja se razlikuje od svih drugih lozinki.
- Koristite softver za detekciju zlonamernih softvera.
- Podesite svoj veb pretraživač tako da ne čuva vaše lozinke (i izbrišite one koje su već sačuvane).

KOME I KAKO PRIJAVITI KRIVIČNO DELO VISOKOTEHNOLOŠKOG KRIMINALA?

Možete prijaviti krivično delo visokotehnološkog kriminala lično policiji ili e-poštom na:

- vtk@beograd.vtk.jt.rs (Posebno tužilaštvo za visokotehnološki kriminal) ili
- ukp@mup.gov.rs (Policija – Služba za borbu protiv organizovanog kriminala)

DOSTAVITE SLEDEĆE INFORMACIJE:

1. Lični podaci:
   - Ime i prezime
   - JMBG (nije obavezno)
   - Adresa
   - Adresa e-pošte
   - Broj mobilnog ili fiksnog telefona
2. Informacije o fizičkom licu/preduzeću koje vam je nanelo štetu
   - Pošaljite sve poznate i/ili raspoložive podatke
3. Novčani gubitak
   - Navedite ukupan iznos koji ste izgubili
   - Da li ste koristili usluge treće strane pri plaćanju kao što su *PayPal* ili *Escrow*?
4. Opis incidenta i dokazi
   - Svojim rečima opišite na koji način ste postali žrtva.
   - Podnesite sve dokaze koje imate.
5. Kontakt za svedoke i druge žrtve
   - Ukoliko postoje svedoci i druge žrtve tog krivičnog dela, dostavite njihove kontakt podatke.

Ova publikacija nastala je uz finansijsku pomoć Evropske unije. Sadržaj publikacije apsolutno izražava stanovišta, mišljenja i stavove projekta *Razvoj elektronskog poslovanja* i ne predstavlja nužno stavove i mišljenja Evropske unije.

Projekat realizuje konzorcijum koji predvodi *Exemplas* u saradnji sa *ACE Consultants, European Profiles, Imorgon, Seidor* i *Teamnet International*

Exemplas ACE europeanprofiles imorgon... seidor teamnet