Andmete õngitsemine

Siit juhendist leiad juhised andmete õngitsemise kohta.

In English

Andmete õngitsemine (ingl *phishing*) on petuskeem, mille eesmärk on meelitada arvutikasutajatelt välja **juurdepääsuandmeid, paroole, krediitkaardinumbreid ja muud tundlikku informatsiooni või saada kontroll kasutaja arvuti üle**.

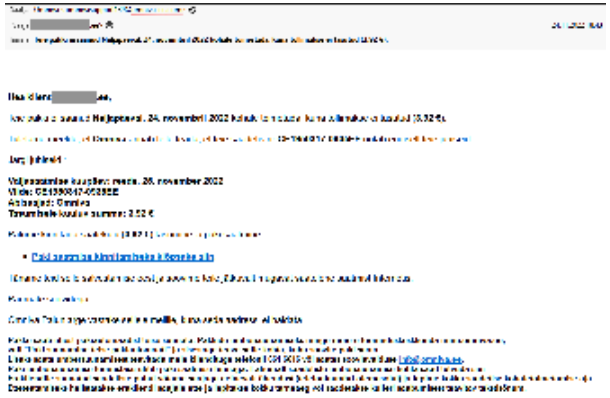
Üldiselt jõuavad petturite andmepüügikatsed kasutajateni meili teel või e-kirjas olevate veebilinkide kaudu, mis võivad välja näha väga tõetruud ja sarnased reaalsete veebilehtedega. Näiteks saadetakse e-kiri sisuga, et teie postkasti maht on täis ja juurdepääsu säilitamiseks tuleb kuskile vajutada.

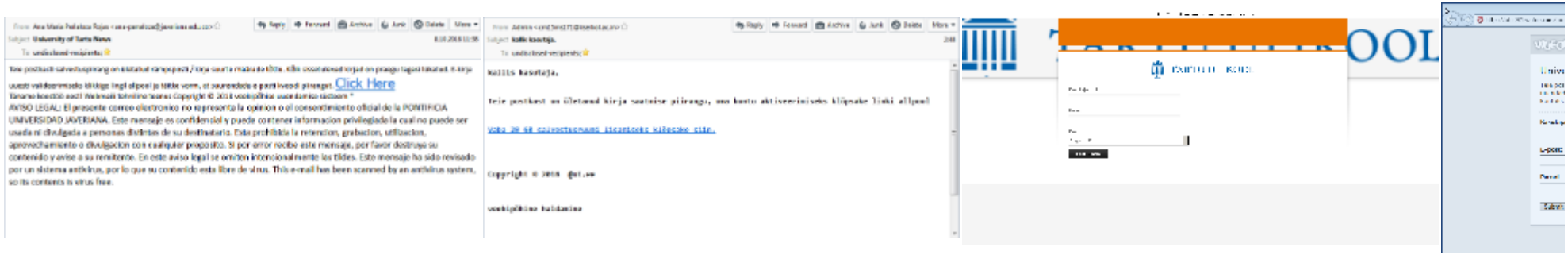
Viimasel ajal on levinud andmete õngitsemine ka telefonikõnede kaudu.

Tihti on kirjad või kõned ähvardava sisuga ja nõuavad kiiret tegutsemist. Samuti on õngitsuskirjad ja kõned enamasti võõrkeelsed,

Tartu Ülikool ei küsi kunagi Teie paroole meili teel!

Juhised





- **Ähvardused ja kiirustamine**. E-kirja saatja või helistaja esitab kellegi teise nimel (tavaliselt politsei, pank) ähvardusi ja nõuab kiirelt tegutsemist. Soovitame sellistele kirjadele mitte vastata ja selline kõne kohe lõpetada ning anda juhtunust kohe arvutiabile teada.
- **Ebakõlad**. E-kirja saatja meiliaadress pole tulnud vastava asutuse domeeniaadressilt või sõnum saadetud nii, et kirja saaja pole aru saada. Tartu Ülikoolis tehtavad suuremad muudatused on eelnevalt teavitatud ja nende kohta saab lugeda TÜ siseveebist. Tartu Ülikooli meiliaadressid lõppevad reeglina @ut.ee.
- **Kahtlased lingid**. Veebileht ei ole vastava asutuse oma ehk lingid on seotud mõne muu domeeniga. Samuti ei kasuta veebileht turvalist ühendust https-protokolli kaudu. Ülikooliga seotud domeeniaadress on reeglina vaid ut.ee lõpuga.
- **Võõrkeelne kiri, õigekirja- ja grammatikavead**. Meilisõnum on ebatavaliselt võõrkeelne, sisaldab on kirja- või keelevigu või on veidralt sõnastatud. Eesti ametiasutused, pangad ning ka ülikooli kirjad ning telefonikõned on tavaliselt eestikeelsed või sisaldavad infot nii eesti kui inglise keeles.

Kui olete andnud oma TÜ kasutajakonto parooli ja muud juurdepääsuandmed võõrastele isikutele, tuleb kohe muuta oma TÜ kasutajakonto parooli keskkonnas https://parool.ut.ee/.

Ühtegi parooli ei tohi korduvalt kasutada! Kui Teil on sama parool kasutusel veel kuskil keskkonnas (Gmail, Facebook jmt), tuleb see esimesel võimalusel ka seal välja vahetada! Vajadusel võtke ühendust arvutiabiga.

Andmepüügipettusest teatamiseks saatke saadud e-kiri edasi aadressil spam@ut.ee ja soovitatavalt manusena. See tagab, et e-kirjaga tulevad kaasa kõik vajalikud kirjapäised, mis on täpsemaks analüüsiks vajalikud. Juhend: E-kirjade saatmine manustena.

Kahtlastest kõnedest andke samuti teada arvutiabile.

- Ärge avage kirju, mis on tulnud tundmatutelt ja kahtlastelt saajatelt.
- Ärge laadige alla tundmatute saatjate kirjadega kaasas olevaid manuseid;
- Ärge klõpsake tundmatute saatjate kirjas olevatel veebilinkidel;
- Ärge kahtlasele kirjale vastake. See julgustab pahalasi uuesti ja paremini proovima.

Kui miski tundub kahtlane, pöörduge alati arvutiabi poole!