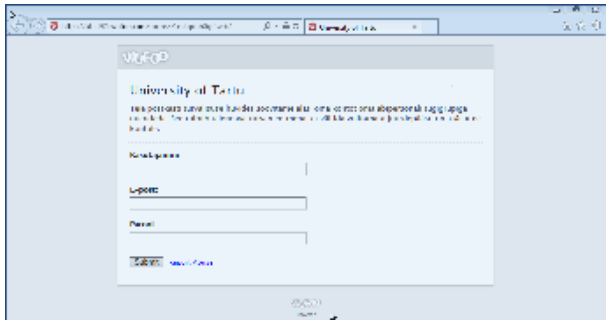
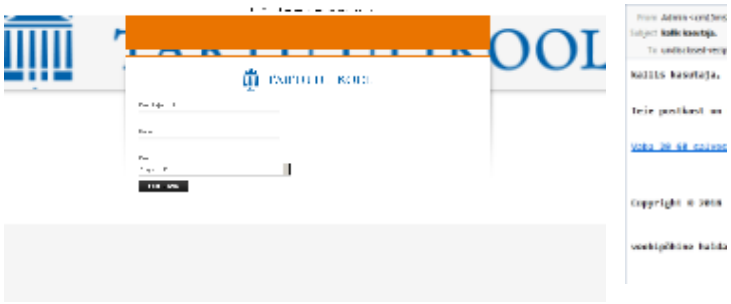
Andmete õngitsemine

Andmete õngitsemine (inglise keeles *phishing*) on petuskeem, mille eesmärk on arvutikasutajatelt **välja meelitada juurdepääsuandmeid, paroole, krediitkaardinumbreid ja muud tundlikku informatsiooni**. Üldiselt jõuavad petturite andmepüügikatsed kasutajateni meili teel või e-kirjas olevate veebilinkide kaudu, mis võivad välja näha väga tõetruud ja sarnased reaalsetele veebilehtedele. Näiteks saadetakse e-kiri sisuga, et teie postkasti maht on täis ja vajutage siia, et juurdepääs säilitada vms.

Tartu Ülikool ei küsi kunagi Teie paroole meili teel!

Näiteid andmepüügikatsetest (veebilehed ja e-kirjad):





Kuidas ära tunda andmepüügikirju?

- **Ebakõlad**. Kui e-kirja saatja meiliaadress pole tulnud @ut.ee aadressilt või sõnum on omakorda saadetud kellelegi salakoopiana. Suuremad muudatused ja tegevused on kooskõlastatud ja kindlasti loetavad ka TÜ siseveebist.
- **Kahtlased lingid**. Kui veebileht ei ole Tartu Ülikooli oma ehk lingid ei ole ut.ee domeeniga. Kui veebileht ei kasuta https protokolli.
- **Õigekirja- ja grammatika vead**. Kui meilisõnumis on kirja- või keelevead.

Kuidas käituda kui olen saanud andmepüügikirja?

Juhul, kui olete andnud oma TÜ kasutajakonto parooli ja muud juurdepääsuandmed võõrastele osapooltele, siis tuleb koheselt muuta oma TÜ kasutajakonto parool keskkonnas: https://parool.ut.ee/. Kindlasti tuleks vältida parooli ristkasutamist ehk kui Teil on sama parool kasutusel veel kuskil keskkonnas (Gmail, Facebook vms), siis tuleb parool vahetada ka seal! Lisainfo ja probleemide korral võtta ühendust Arvutiabiga.

Andmepüügipettusest teatamine: tuleb see e-kiri edasi saata aadressil arvutiabi@ut.ee ja soovitatavalt edasi saata manusena (*Forward as Attachment*).

- ei tohi kirju avada, mis on tulnud tundmatutelt ja kahtlastelt saajatelt;
- ei tohi alla laadida kirjades kaasas olevaid manuseid;
- ei tohi avada kirjas olevaid veebilinke;
- ei tohi kirjale vastata.

Kui miski tundub kahtlane, võite alati Arvutiabist üle küsida!