Funded by the
Erasmus+ Programme
of the European Union

Küberrünnakute mõistmise ja nendega toimetuleku ülevaade

Alusteadmised e-turvalisusest

Safeguarding against Phishing in the age of 4th Industrial Revolution
www.cyberphish.eu
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

CyberPhish
Safeguarding your digital future

Õppe-eesmärgid

Selgitage e-turvalisuse kontseptsiooni ja küberohtude ennetava lähenemise tähtsust küberhügieeni kontseptsiooni kaudu

Funded by the Erasmus+ Programme of the European Union

Õpilase töökoormus

Loengud	0,5 h
Audio- ja videomaterjal	0,5 h
Juhtumiuuringud	0,5 h
Lisalugemine	1 h
Eksamiks valmistumine	0,5 h

Funded by the
Erasmus+ Programme
of the European Union

Loenguteemad

Infosisu ja vajadus sisu turvata

Intellektuaalne omand; isiklikud andmed; identiteet

Kuidas pahavara seadmesse satub?

Mis on identiteedi-varguste ja isikuandmete avaldamise põhjused ja tagajärjed?

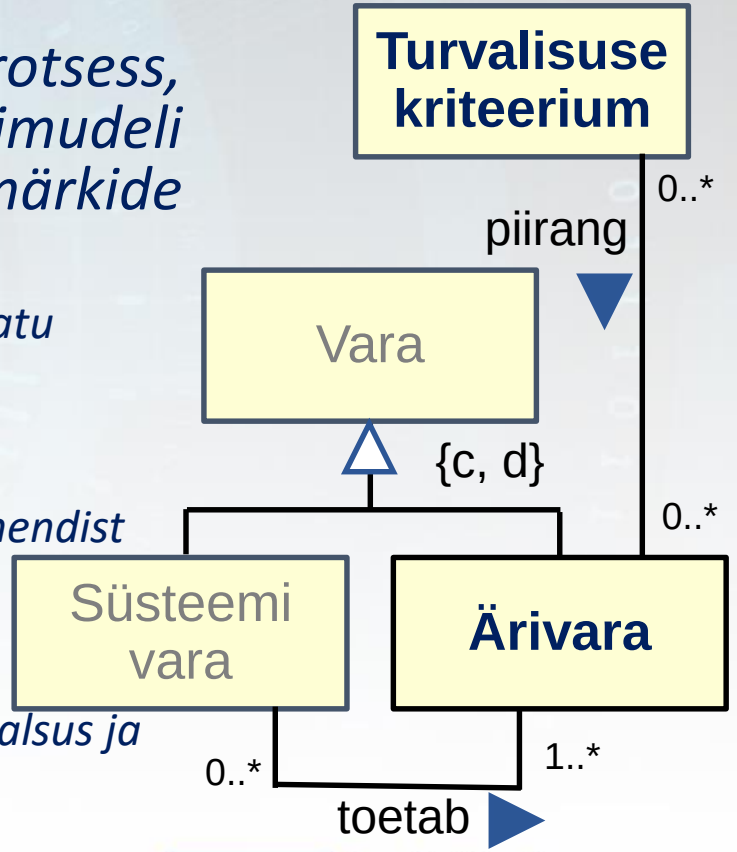
CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Ärivara ja Turvalisuse kriteeriumid

Avalik info *vs* Privaatne informatsioon

- **Ärivara:** *organisatsiooni äritegevusele omane teave, protsess, oskused, mis omavad organisatsiooni jaoks ärimudeli seisukohalt väärtust ja on vajalikud äri eesmärkide saavutamiseks*
  - **Konfidentsiaalsus:** *Teabe omadus olla kättesaamatu või paljastamatu volitatamata isikutele ja protsessidele. Üks kolmest turvalisuse põhikategooriast (teised kaks on käideldavus ja terviklus)*
  - **Integrity:** *Lubamatute muudatuste puudumine, hõlmab ka autentsust ja salgamatust, üks teabe turvalisuse kolmest põhikomponendist levinuimas turvamudelis*
  - **Käideldavus:** *Teabe, IT-süsteemide, inimeste, protsesside teovõime ja kättesaadavus volitatule siis, kui ta neid vajab. Üks kolmest turvalisuse põhikategooriast (teised kaks on konfidentsiaalsus ja terviklus)*

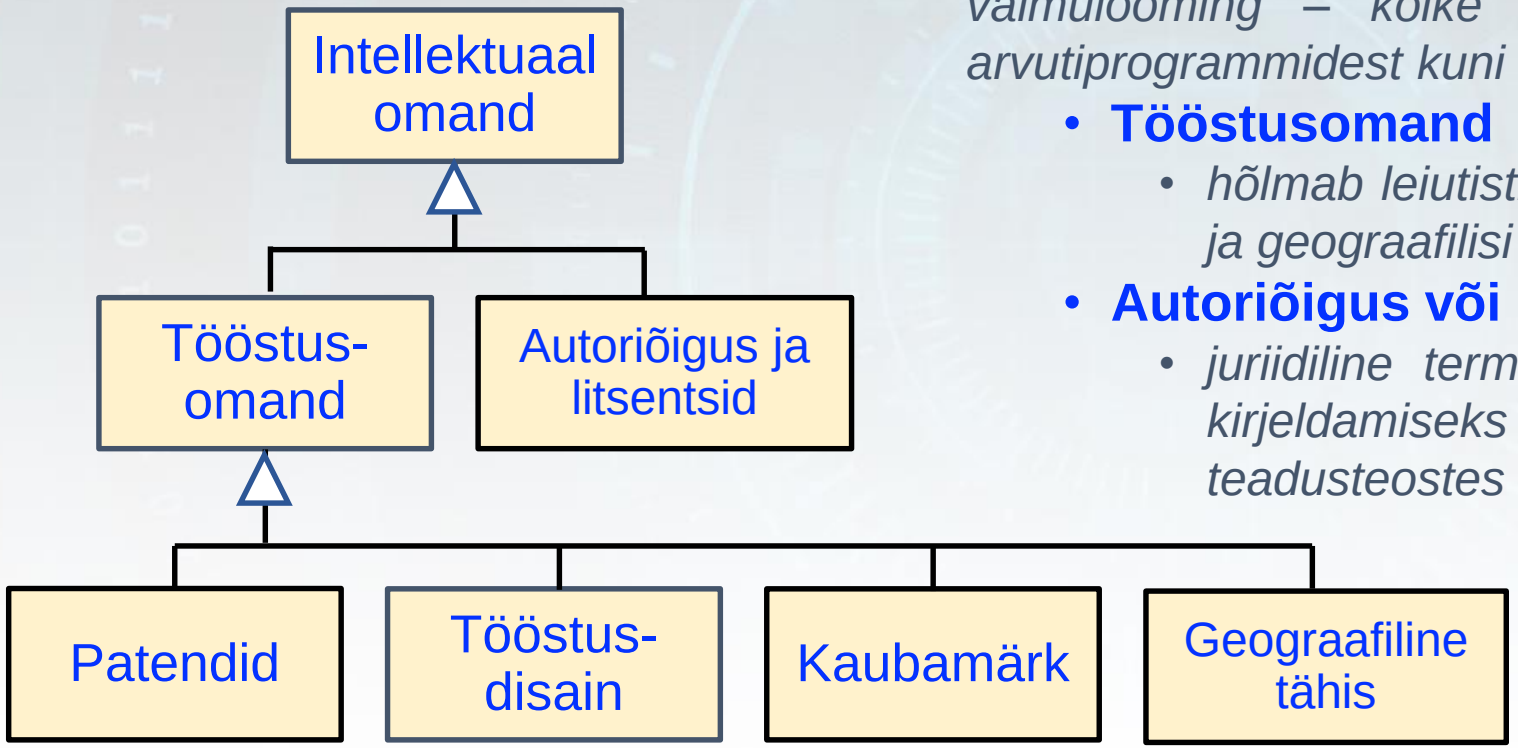


[*Dubois at al., 2010*]

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Intellektuaalne omand



Intellektuaalne omand

vaimulooming – kõike alates kunstiteostest kuni leiutisteni, arvutiprogrammidest kuni kaubamärkide ja muude ärimärkideni

- **Tööstusomand**
  - *hõlmab leiutisti, tööstusdisaini lahendusi, kaubamärke ja geograafilisi tähistusi*
- **Autoriõigus või autori õigus**
  - *juriidiline termin, mida kasutatakse autorite õiguste kirjeldamiseks oma kirjandus-, kunsti- ja teadusteostes*

WIPO: What is intellectual property? https://www.wipo.int/about-ip/en/

Isiklikud andmed

‘**Isiklikud andmed**’ *mis tahes teave tuvastatud või tuvastatava füüsilise isiku (andmesubjekti) kohta; tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige viidates identifikaatorile, nagu nimi, identifitseerimisnumber, asukohaandmed, võrguidentifikaator või üks või mitu tegurit, mis on iseloomulikud selle füüsilise isiku füüsilisele, füsioloogilisele, geneetilisele, vaimsele, majanduslikule, kultuurilisele või sotsiaalsele identiteedile.*

EU General Data Protection Regulation.
URL: https://eur-lex.europa.eu/legal-content/ EN/TXT/?uri=uriserv:OJ.L.2016.119.01.0001.01.ENG

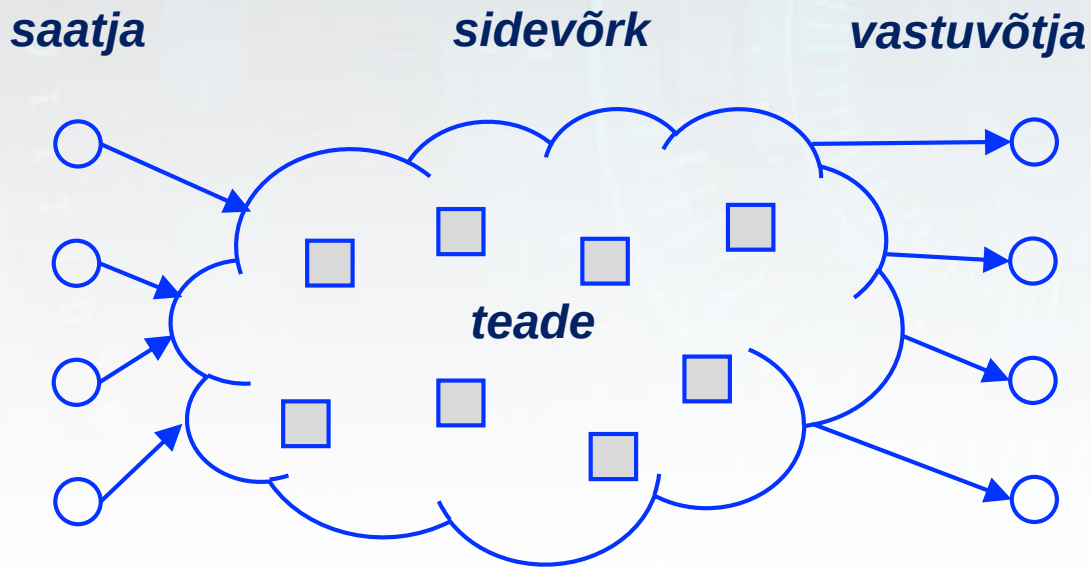
This Photo by Unknown Author is licensed under CC BY-SA

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Identiteet

- **Identiteet** *on mis tahes üksikisiku atribuutide väärtuste alamhulk, mis identifitseerib selle isiku piisavalt mis tahes isikute hulgas*
  - *Nimi, identifikaatorid, digitaalsed pseudonüümid, aadress*, jne.



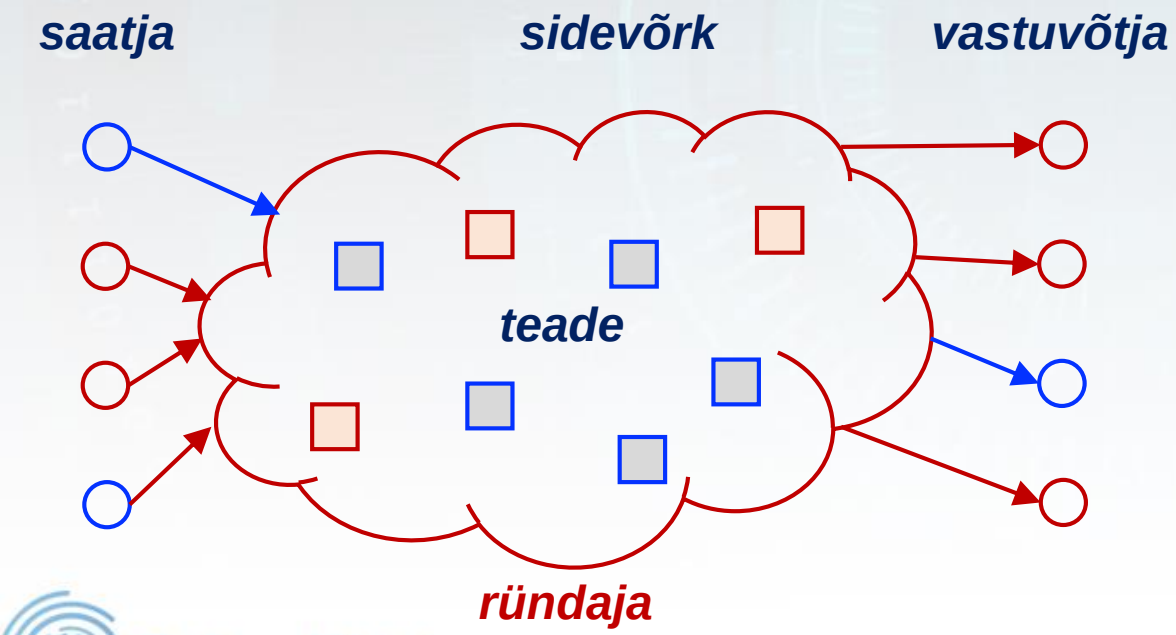
- **Anonüümsus** *tähendab, et subjekt ei ole anonüümsuskomplekti hulgas tuvastatav, st kõik subjektid*
- **Tuvastamatus** *huvipakkuva eseme olemasolu suhtes tähendab, et ründaja ei suuda eristada, kas huvipakkuv objekt on olemas või mitte*
- **Ühendamatus** *Kahe või enama huvipakkuva üksuse olemasolu tähendab, et ründaja ei suuda piisavalt eristada, kas need on seotud või mitte*

[*Pfitzmann and Hansen, 2010*]

Funded by the Erasmus+ Programme of the European Union

Identiteet

- **Identiteet** *on mis tahes üksikisiku atribuutide väärtuste alamhulk, mis identifitseerib selle isiku piisavalt mis tahes isikute hulgas*
  - *Nimi, identifikaatorid, digitaalsed pseudonüümid, aadress*, jne.



- **Anonüümsus** *tähendab, et subjekt ei ole anonüümsuskomplekti hulgas tuvastatav, st kõik subjektid*
- **Tuvastamatus** *huvipakkuva eseme olemasolu suhtes tähendab, et ründaja ei suuda eristada, kas huvipakkuv objekt on olemas või mitte*
- **Ühendamatus** *Kahe või enama huvipakkuva üksuse olemasolu tähendab, et ründaja ei suuda piisavalt eristada, kas need on seotud või mitte*

[Pfitzmann and Hansen, 2010]

Kuidas ründetarkvara seadmesse satub

[*Anderson, 2008*]

Ründaja unistus:

- Hankida tohutul hulgal arvutusvõimsust ja proovida KÕIKi võimalikud krüptitud võtme kombinatsioone
- Paigaldada **klahviluger** *või* **trooja** tarkvara ohvri arvutisse
  - *Kasutate Internetiga ühendatud seadmetes aegunud (ebaturvalist) tarkvara*
  - *Installite kaugjuhtimist võimaldava pahavara*
  - *Dekrüpteeritud sõnumit saab lugeda arvuti mälust või kõvakettalt*

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kuidas saada kellegi parool teada?

[*Anderson, 2008*]

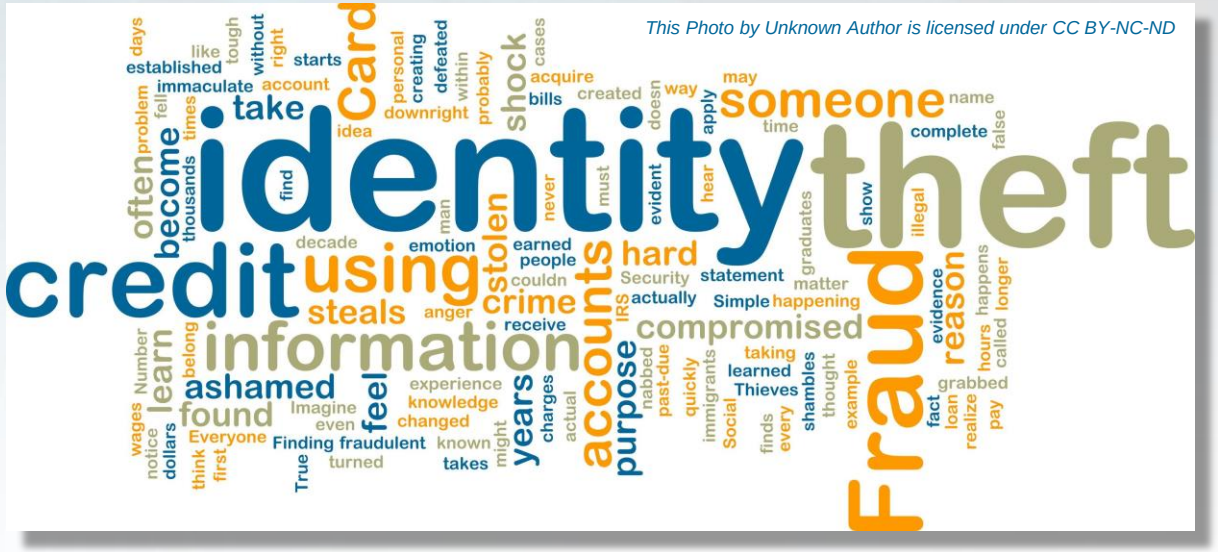
- Arvame ära parooli
- Küsime ohvrilt tema parooli
  - **https://youtu.be/opRMrEfAIiI**
  - **https://youtu.be/UzvPP6_LRHc**

password	*master*
123456	*sunshine*
12345678	*ashley*
qwerty	*bailey*
abc123	*passw0rd*
monkey	*shadow*
1234567	*123123*
letmein	*654321*
trustno1	*superman*
dragon	*qazwsx*
baseball	*michael*
111111	*football*
Iloveyou	

Funded by the Erasmus+ Programme of the European Union

identiteedi- ja isikuandmete varguste põhjused

- Ebapiisav turvakoolitus
- (Asjakohaste) turvapoliitikate puudumine
- Teadmatus
  - *mitmed organisatsioonilised üksused*
- Sotsiaalsed ründed
  - *Empaatia aidata hädas olijat*
- Lihtne juurdepääs teabele
  - *emaili kasutajatunnused*
  - *telefoninumbrid*



Küberrünnakute Tagajärjed

- **Sümptomid**
  - *Suurenenud protsessori kasutus*
  - *Seadme või veebibrauseri aeglane kiirus*
  - *Probleemid võrkudega ühenduse loomisel*
  - *Külmumine või krahh*
  - *Muudetud või kustutatud failid*
  - *Kummaliste failide, programmide või töölauaikoonide ilmumine*
  - *Programmid töötavad, lülituvad välja või konfigureerivad end ümber*
  - *Seadme kummaline käitumine*
  - *E-kirjad/sõnumid saadetakse automaatselt ja kasutaja teadmata*

- Maine kahjustamine
- Petturlik teabekasutus
- Teabe kadu
- Privaatsuse kaotus
- Majanduslikud kahjud
- Kohtuasjad ja kahjutasud
- Tööseisak
- Sabotaaž ja terrorismiohud

Funded by the Erasmus+ Programme of the European Union

Kokkuvõte

- **Ärivarad:**
  - *Intellektuaalomand, isikuandmed ja identiteet*
  - *Turvavajadus: konfidentsiaalsus, terviklikkus, kättesaadavus*
- Pahatahtliku tarkvara seadmesse sattumise **viisid**
- Identiteedivarguste ja isikuandmete avalikustamise **põhjused** ja **tagajärjed**

Funded by the Erasmus+ Programme of the European Union

Ülesanded

Arutage, mis on **identifitseeritavus**, **seostatavus** ja **tuvastatavus** ründaja vaatenurgast

Arutage, kuidas seadet **ründetarkvara** eest **kaitsta**

näiteks: viirused, klahvilugerid, trooja, botned jne

Kas olete kunagi kogenud seadme **"vale käitumise" sümptomeid**? Kuidas sa need **parandasid**?

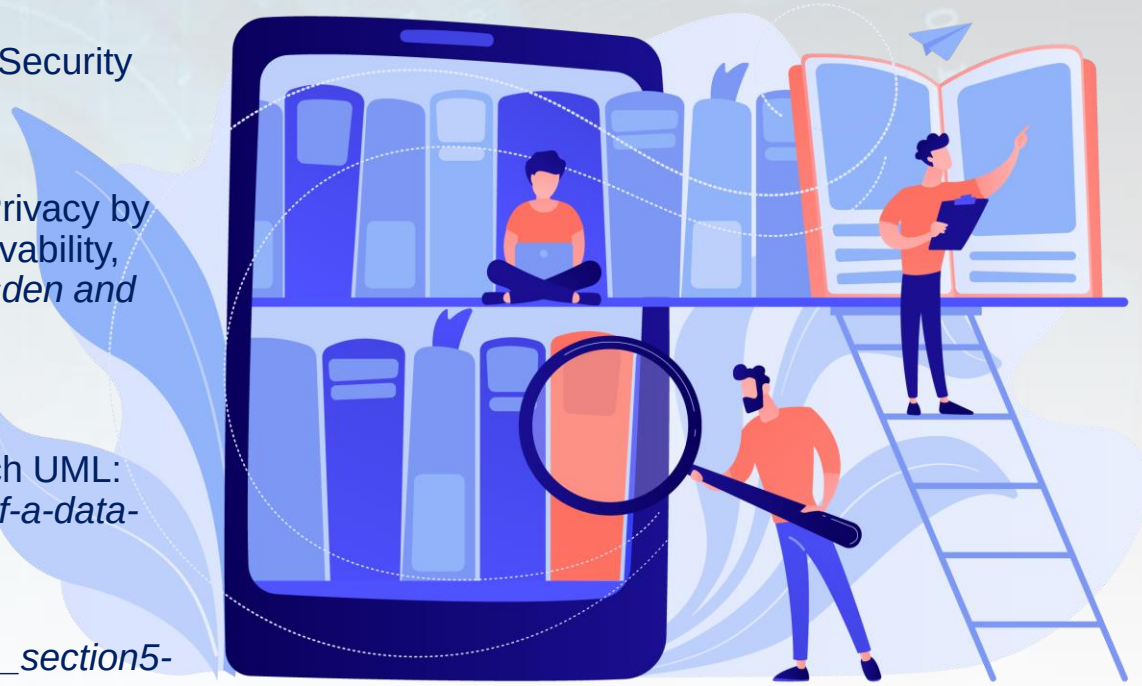
Lisalugemine

Selle loengu ettevalmistamisel kasutatud materjal

- **Anderson, R.** (2008) Security Engineering: A Guide to Building Dependable Distributed Systems, *2nd edn. Wiley, New York*
- **Dubois E., Heymans P., Mayer N., Matulevičius R.** (2010) A Systematic Approach to Define the Domain of Information System Security Risk Management. *Intentional Perspectives on Information Systems Engineering 2010: 289-306*
- **Pfitzmann, A., Hansen, M.** (2010) A Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. *Technical Report, TU Dresden and ULD Kiel*

Kasulikud lingid

- **Strawbridge G.** (2020) 5 Damaging Consequences Of A Data Breach UML: *https://www.metacompliance.com/blog/5-damaging-consequences-of-a-data-breach/*
- **State of New Jersey 2014 Hazard Mitigation Plan**. URL: *https://www.state.nj.us/njoem/programs/pdf/mitigation2014b/mit2014_section5-23.pdf*
- **World Intellectual Property Organisation**, What is intellectual property? URL: *https://www.wipo.int/about-ip/en/*



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Lühivideod

- Understanding intellectual property
  - ***https://youtu.be/UqZJPuyK9VY***
- What is personal data under GDPR?
  - ***https://youtu.be/qJX3fbq3fOg***
- Intellectual Property Theft
  - ***https://youtu.be/0y0KV0B1v10***
- The most horrific case of identity theft
  - ***https://youtu.be/CJ40tAm8cTE***
- What can happen to your personal data online?
  - ***https://youtu.be/v4IIH3sJlMc***

Tänan kuulamast!