
UPPLÝSINGAÖRYGGI
HVER BER ÁBYRÐ?
SKÝ 2018

YFIRLIT

Hver ber ábyrgð?

Tækni

Öryggismenning

Öryggisvitund notenda

HVER BER ÁBYRGÐ?

Tækni = IT

- **IT** hefur hingað til borið ábyrgð á upplýsingaöryggi og þurft að kaupa sig út úr hættunum
- Auðvelt að fjárfesta á röngum stöðum með litlum ávinningi

Öryggismenning = STJÓRNENDUR

- Upplýsingaöryggi þarf að vera eins og annað öryggi, partur af stefnu og menningu fyrirtækis
- Hér bera **allir stjórnendur** ábyrgð og þurfa að leggja sitt af mörkum
- GDPR er til þess fallið að færa ábyrgðina til fyrirtækisins – nýtum það

Öryggisvitund notenda = ALLIR

- Notandinn er veikasti hlekkurinn í öryggiskeðjunni og er hann því iðulega helsta skotmark tölvuþrjóta
- Notendur þurfa að skilja tæknina betur og vita hvað ber að varast
- Hér bera **allir notendur** ábyrgð

TÆKNI – IT BUDGET

Upplýsingaöryggi verður áfram að hluta vandamál IT og það þarf budget til að kaupa nýja tækni til að leysa málin

Rannsókn IDC á 200 fyrirtækjum í Canada sýndi að:

- 23% settu minna en 6% af IT budget í upplýsingaöryggi (defeatists)
- 37% settu minna en 8% af IT budget í upplýsingaöryggi (denialists)

Alls 6 af 10 fyrirtækjum að fjárfesta undir meðaltali í upplýsingaöryggi. Þau reyndust með lágan öryggisþroska (maturity rating <3) og öryggisfrávik yfir meðaltali.

Top 40% fyrirtækin voru með öryggisfrávik undir meðaltali og hærri þroska. Þau skiptust í tvo hópa:

- Realists með 14% af IT budget og ágætis öryggi en vildu gera betur
- Egoists með 12% af IT budget voru **á toppnum** með mestan þroska (4-5) og besta árangurinn

TÆKNI – IT BUDGET

Hvers vegna var besti hópurinn ekki með mestu fjárfestinguna ?

- Meiri þroski skilar sér oft í lægri fjárfestingum með því að nota betri ferli
- Bætt innkaupaferli geta t.d. skilað lægri kostnaði með auknum kröfum til framleiðenda
- Sniðganga léleg óörugg kerfi og setja minni pening í að prófa þau og verja
- Einnig færist kostnaður út til fyrirtækisins sem hluti af öryggismenningu þess
  - Þjálfun
  - Æfingar
  - Forvarnir

Við kaupum okkur ekki út úr vandanum með tólum einum saman

https://www.theregister.co.uk/2015/08/18/responsibility_for_it_security/

TÆKNI – EINFALDAR LAUSNIR

Einfalda lausnir eins og hægt er til að berjast á sem fæstum vígstöðvum

- Ef það er allt í drasli, olía, gas og tuskur í bílskúrnum.... ekki kaupa bara annan reykskynjara

Hafa grunnþjónustur í lagi með góðu skipulagi

- Uppfærslur þurfa að vera í topp standi
- Vírusvarnir og spam varnir í gangi
- Umgengni, lykilorðapolicyur og 2FA
- Skilríkjavæðing á búnaði (enrollment)

Þá skiptir máli að spyrja rétta aðila góðra spurninga:

- Hvað gerist ef við gerum þetta ekki?
- Getum við leyst þetta á annan hátt?
- Getum við breytt vinnulagi eða arkitektúr?
- Getum við fært eða einfaldað varnarlínuna?

ÖRYGGISMENNING

Hver er öryggismenning fyrirtækisins?

Er öryggisstjóri? Er upplýsingaöryggisstjóri?

Er verið að nota „secure coding“ í þróun? (t.d. OWASP)

Er regluleg kennsla fyrir alla í upplýsingaöryggi?

Eru reglulegar æfingar eða veikleikaprófanir?

Er til samskiptaáætlun og viðbragðsáætlun?

Er verið að fylgja ISO27001?

Getum lært mikið af því hversu vel hefur tekist í framþróun á raunlægu öryggi á vinnustöðum seinustu ár.

Það er ekki lengur púkó að vera öruggur

ÖRYGGISMENNING

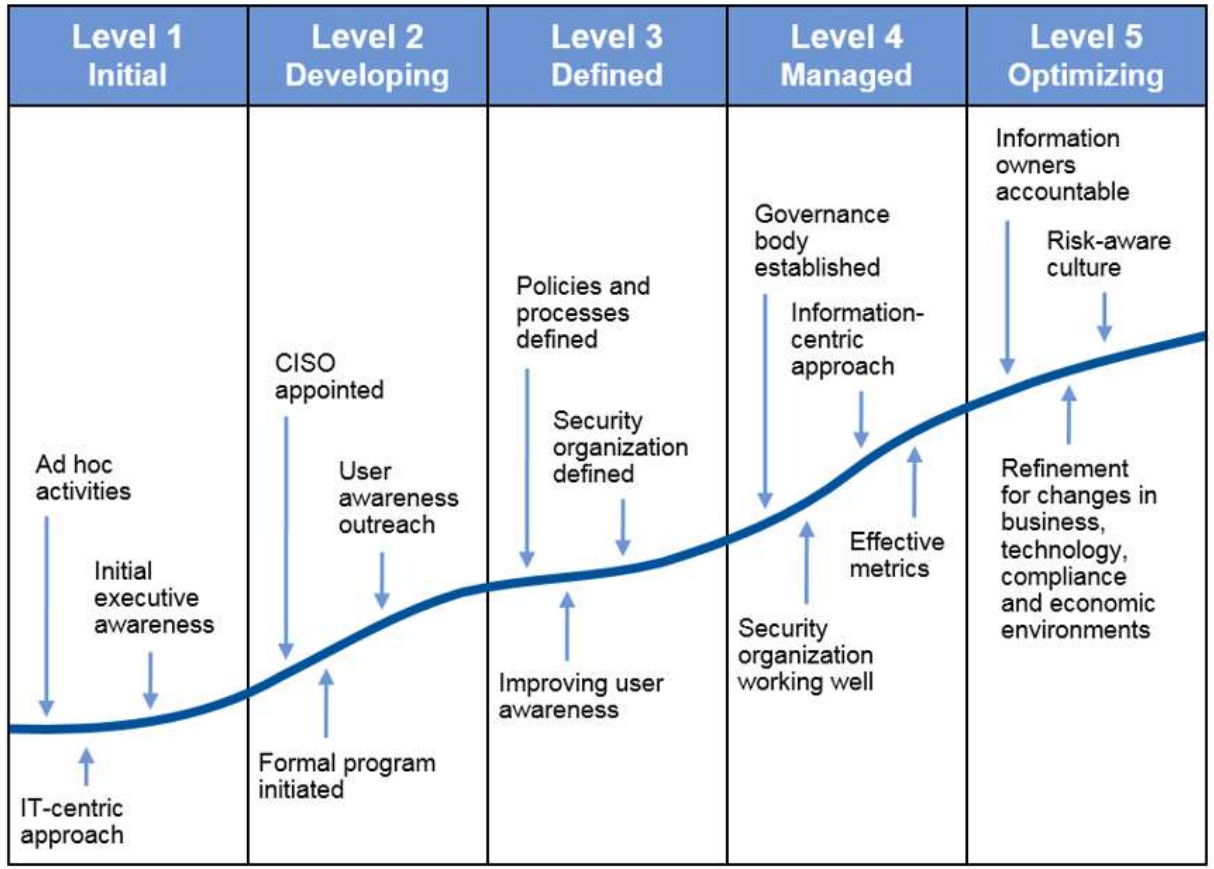
Gartner „ITScore for Information Security“

Eitt tólið sem hægt er að nota til að skilgreina öryggisþroska og ferðalagið

Þetta er fyrst og fremst sameiginlegt ábyrgðarhlutverk stjórnenda fyrirtækis

IT þarf að aðstoða við þessa þróun, ekki bara gera Level 1 dýrara

GDPR hjálpar fyrirtækjum hér ef því er tekið fagnandi og látið keyra framþróun



Source: Gartner (February 2016)

ÖRYGGISVITUND NOTENDA

Upplýsa alla stjórnendur um grunnþætti upplýsingaöryggis

- Hlutverkin, öryggisráð, ferlin sem þarf ofl.
- Taka út frá GDPR og maturity módelum

Kynna almennt upplýsingaöryggi fyrir öllum starfsmönnum og viðhalda stöðugum áróðri

Hverjar eru hætturnar í umhverfinu?

- Þjófnaður
- Hacking
- Phishing / spear phishing
- Malware
- Gögn á glámbekk

Kenna notendum að sjá hætturnar og hvernig þeir geta varist þeim?

SAMANTEKT

Öryggismenning:

- Keyra af stað með stjórnendum og tryggja fullan stuðning
- Nota GDPR sem drifkraft

Öryggisvitund:

- Byggja upp nauðsynlega þekkingu
- Festa regluverk í sessi með stöðugum umbótum og markaðssetningu
- Taka upp mælingar

Tækni:

- Fylgja eftir með réttum tólum og tækjum
- Leita að einföldun lausna og henda gömlum lausnum

ÞÚ BERÐ ÁBYRGÐ!

YFIRLIT

Öryggi gagna

Físískt aðgengi

Stýrikerfi

Net og internet

Phishing

Malware

5 einfaldar reglur

ÖRYGGI GAGNA

Megin leiðir að gögnunum

Fá vélina í hendurnar

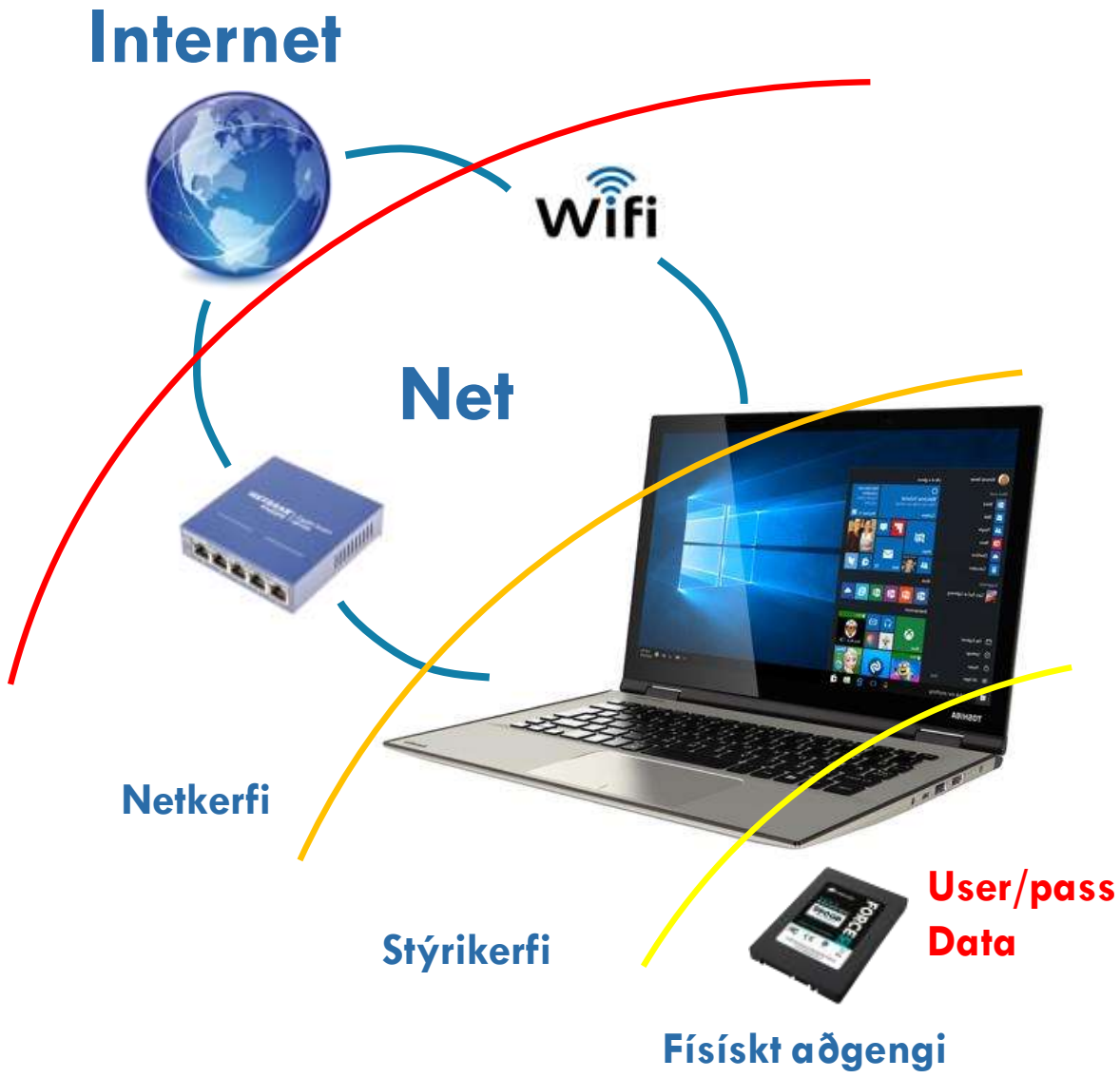
- Setjast við lyklaborðið
- Steeling and hacking

Hlera vélina á neti og nýta veikleika

- Hacking
- Setja upp Malware - Óværur

Fá notandann til að afhenda þau á Internetinu

- **Phishing**
- Setja upp Malware – Óværur
- Láta notanda sækja sjálfur



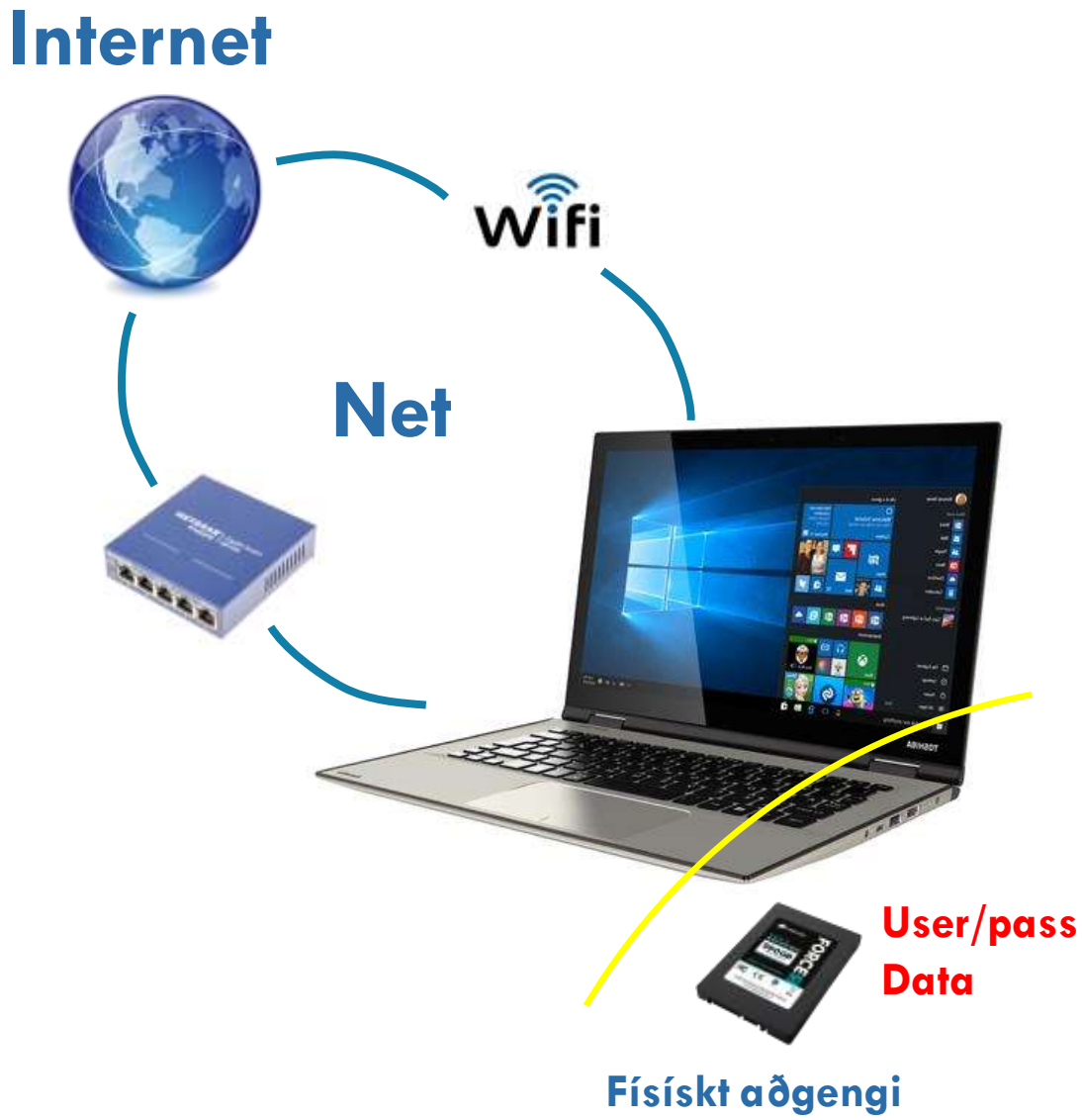
FÍSÍSKT AÐGENGI

Umgengni

- Tryggja aðgang að vél
- Læsa vél
- Ekki láta stela vélinni á ferðalögum
- Ekki gefa frá sér lykilorð

Tæknilegar varnir

- Dulkóða diska
- Læsing stýrikerfis
- Lykilorðareglur



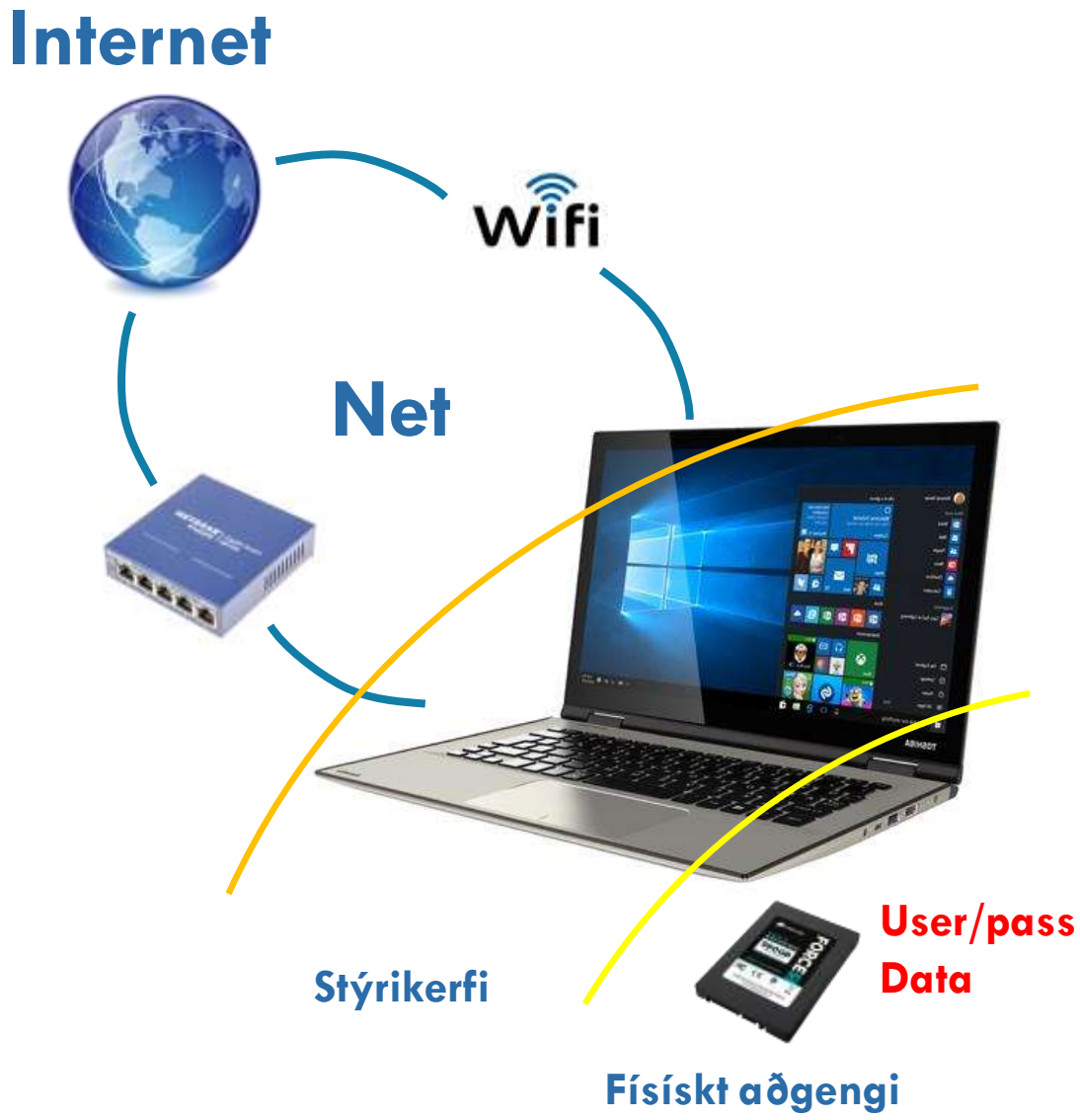
STÝRIKERFI

Umgengni

- Setja ekki upp hugbúnað á vélinni
- Slökkva ekki á vörnum
- Fresta ekki uppfærslum

Tæknilegar varnir

- Regluleg uppfærsla stýrikerfis og hugbúnaðar
- Virkar vírusvarnir
- Virkar innbrotavarnir



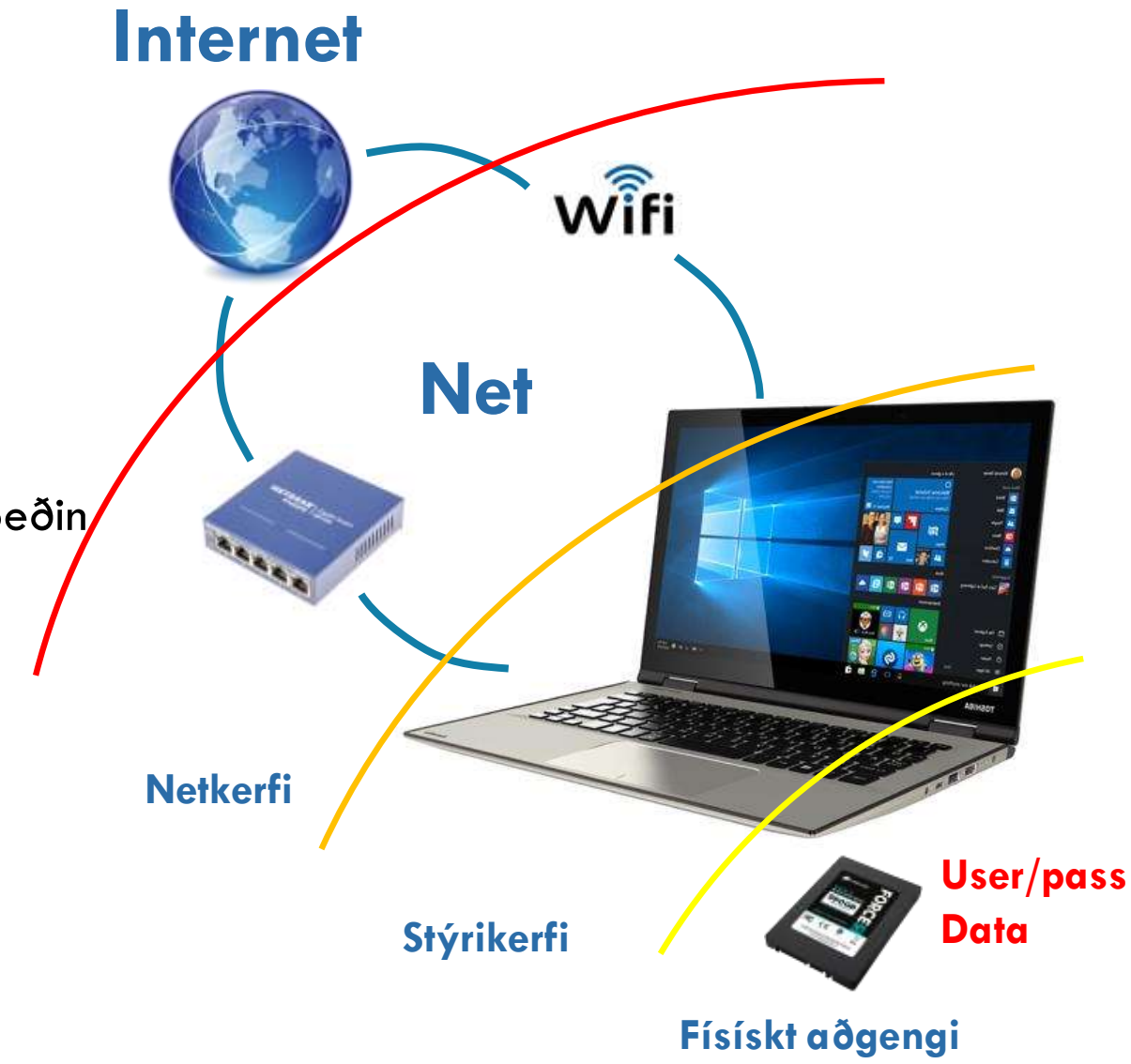
NET OG INTERNET

Umgengni

- Hvað er PHISHING?
- Smella ekki á bull linka
- Gefa aldrei upp lykilorð og pass ef maður er beðin um það
- Setja ekki upp vafasaman hugbúnað
- Fara ekki á vafasamar síður
- Lána ekki vélina

Tæknilegt

- Reyna að tryggja öll samskipti með https
- Nota VPN til að verja vél og samskipti



PHISHING

Sú sviksamlega starfsemi að senda dulbúna tölvupósta undir merkjum virðulegra fyrirtækja í þeim tilgangi að fá einstaklinga til að gefa upp persónulegar upplýsingar á borð við lykilorð og kreditkortaupplýsingar

Þessir póstar senda mann oft inn á síður sem líta nákvæmlega eins út og vefsíður fyrirtækisins

ÞEKKJA PHISHING PÓSTA OG SÍÐUR

5 EINFALDAR REGLUR

Ekki smella á hlekki í óvæntum tölvupósti

Athugaðu hvert slóðin á hlekk vísar

Ekki opna viðhengi úr óvæntum tölvuósti

Uppfærðu hugbúnað á tölvum

Notaðu mismunandi lykilorð á miðlum

ÞÚ SKIPTIR ÖLLU MÁLI !