Jákvæð öryggismenning

Styrkjum mannlega eldvegginn

Guðrún Valdís Jónsdóttir
Öryggissérfræðingur hjá Syndis

Öryggismenning

- Menning er í erfðaefni fyrirtækja
- Ósjálfrátt, þurfum ekki að hugsa um það
- Það sem fólk gerir þegar enginn er að horfa
- Velja lykilorð, lykilorðabankar, tilkynningar, fylgja reglum, o.s.frv.

Jákvæð öryggismenning

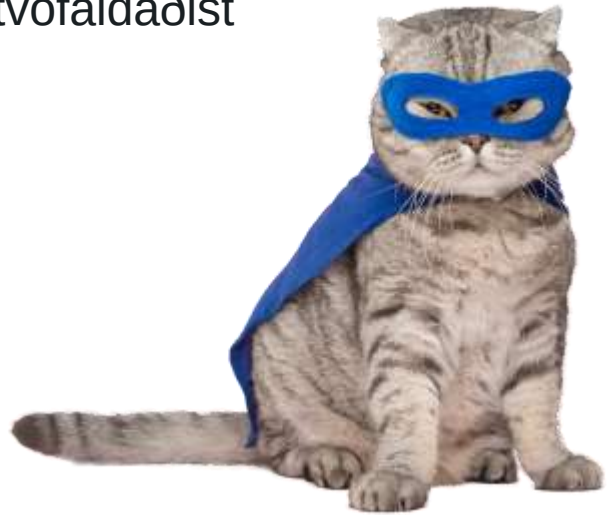
- Starfsfólk finnur til trausts og sanngirni
- Fólk er mótiverað af því að vilja gera vel

- Snúa hugmyndum fólks um öryggi
- Breyta hvernig fólk hugsar og hverju það trúir
- Fá fólkið með okkur í lið

Af hverju öryggismenning?

- 85% öryggisbresta 2021 fólu í sér mannlegan þátt[1]
- Fjárfesting í öryggismenningu borgar sig

- Fjöldi lykilorða stolið í vefveiðiherferðum helmingaðist
- Fjöldi tilkynninga um vefveiðipósta tvöfaldaðist
- Notkun lykilorðabanka þrefaldaðist[2]



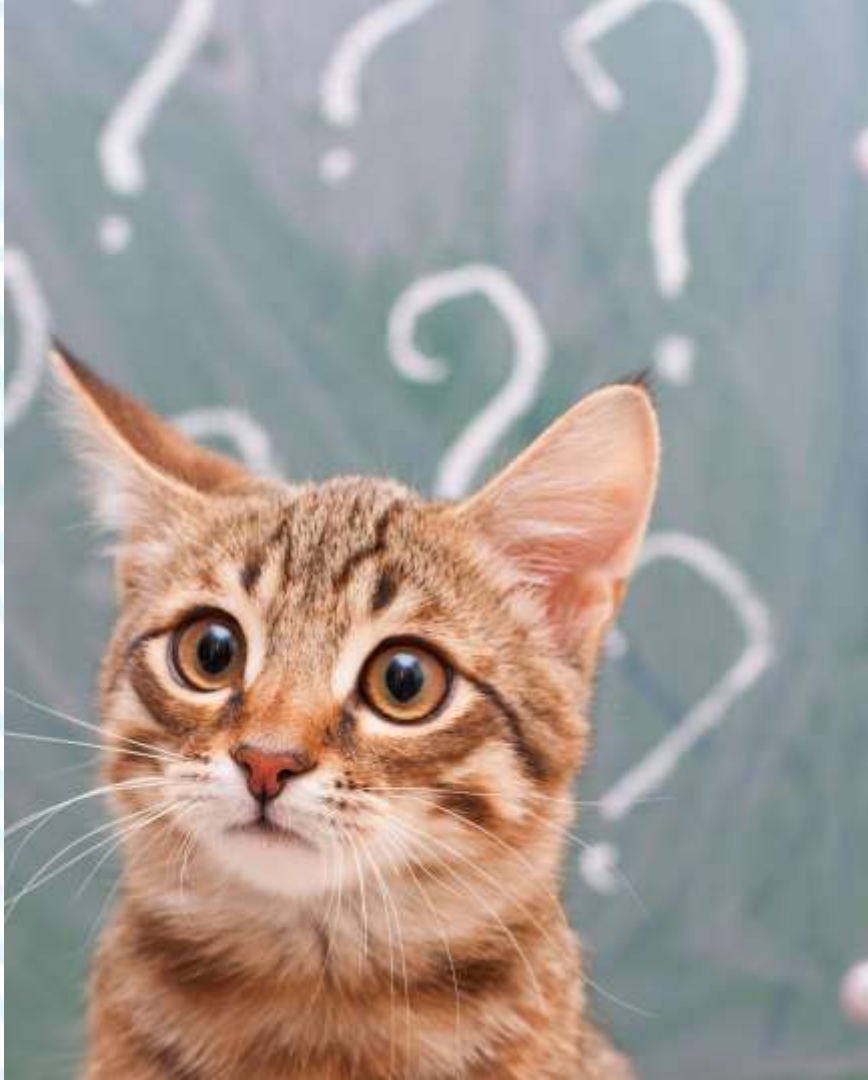
[1] 2021 Data Breach Investigations Report, Verizon, https://www.verizon.com/business/resources/reports/dbir/

[2] Building a Security Propaganda Machine: The Cybersecurity Culture of Verizon Media, https://cams.mit.edu/wp-content/uploads/Verizon-Media-CyberCulture-Paper.pdf

Árangur

- Margar tilkynningar um eigin atvik
- Fólk ræðir vafasaman póst sín á milli yfir hádegismat
- Nýtt starfsfólk sér strax hvað er ásættanleg hegðun
- Góð mæting á öryggistengda viðburði
- Fólk hugsar hlýtt til öryggisstjórans

En Guðrún,
hvernig??



Öryggisstjórar

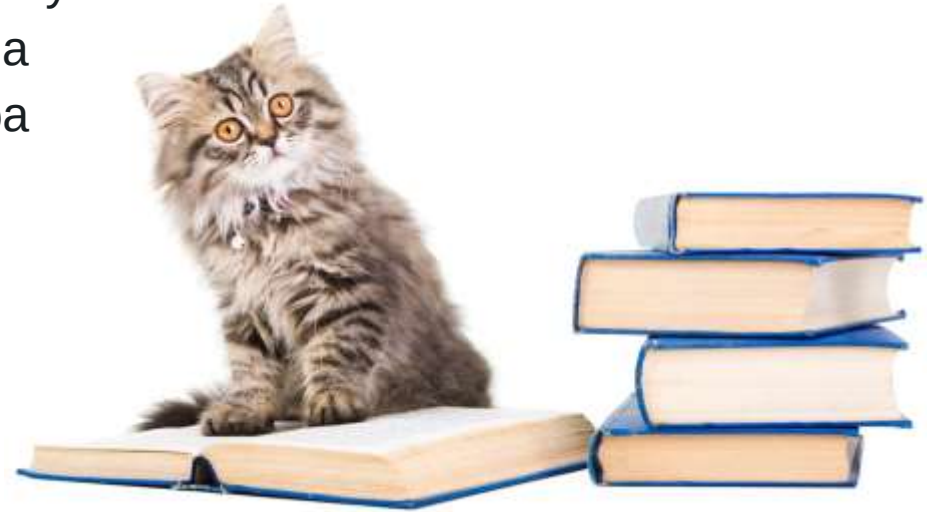
- Vera mjög aðgengileg öðru starfsfólki
- Nýta hvert tækifæri: fréttir og umræðu í samfélaginu, starfsmannafundi, matsalinn, o.s.frv.
- Starfsfólkið hefur alltaf rétt fyrir sér
- Svara öllum spurningum og tilkynningum

Öryggisstjórar

- Mikilvægt að stjórnendur séu stuðningsríkir
- Finna „áhrifavalda” innan mismunandi deilda
- Gera réttu hlutina auðvelda fyrir starfsfólk, t.d. setja upp lykilorðabanka á allar vélar sem er stjórnað af fyrirtækinu
- Hvatar - verðlauna þá sem gera vel

Þjálfun

- Búa til þjálfunaráætlun varðandi öryggismál
  - Nýliðaþjálfun
  - Regluleg þjálfun
  - Hvað skal rætt og hvenær
- Sérsníða efnið að ykkar fyrirtæki
- Uppfæra efnið reglulega
- Fræða, ekki bara hræða
- Gaman!



Vefveiðar (phishing)

- Breytum aðferðafræðinni
- Undirbúningur
  - ~~**enginn?**~~
- Mælingar
  - ~~**hve margir féllu fyrir póstinum**~~
- Lærdómur
  - ~~**útvaldir sendir í meiri þjálfun**~~
  - ~~**refsing?**~~

Vefveiðar - undirbúningur

- Gefum starfsfólki tól til að greina vefveiðipósta
- „Á næstu 3 vikum verður vefveiðipróf”
- Gera skýrt að öryggisstjórinn er ekki illkvittinn, erum öll saman í liði
- Verið að prófa viðbrögðin

Vefveiðar - mælingar

- Rangur mælikvarði að skoða hversu margir „falla”
  - Auðvelt að búa til svínslegan póst
- Nýr mælikvarði: **hve margir tilkynna**
- Taka vel í allar tilkynningar

Vefveiðar - lærdómur

- Draga fram jákvæðu niðurstöðurnar
- Ekki skamma
- Skilja hvers vegna sumir tilkynntu ekki

100% af þeim sem smelltu á hlekkinn tilkynntu CISO

27 áframsendu grunsamlega póstinn á öryggisstjóra

Miklu fleiri sem tilkynntu núna en síðast

Takk!

SYNDIS
Creative[in]Security