



LÖGREGLAN Á HÖFUÐBORGARSVÆÐINU



Tölvupóstsvindl – fyrirmælafölsun

Áhættuhópar: Félagasamtök, íþróttafélög, stofnanir, fyrirtæki.

Þetta svindl er afar algengt og miðar helst gegn fyrirtækjum og félagasamtökum. Þetta hefur gegnið yfir í nokkur ár og það hefur verið fjallað um það í fjölmiðlum. Netsvindlið fer þannig fram að gjaldkeri virðist fá tölvupóst frá formanni félagasamtaka/fyrirtækis um að framkvæma greiðslu. Pósturinn er oft sannfærandi og á yfirborðinu lítur allt vel út. Vandinn er að sendandinn er allt annar og greiðslufyrirmælin eru sviksamleg. En á meðan samskiptin eru gerð með að svara upphaflega tölvupóstinum þá eru samskiptin alltaf við glæpamennina:

Dæmi um samskipti (búið er að breyta texta með XXXX til að hylja persónuupplýsingar)

From: johannXXXXXXXXXX
Sent: 21. september 2019 13:44
To: GísliXXXXXXXXXX
Subject: Re: Brýnt verkefni

Gísli

Hér að neðan finnur þú nauðsynlegar upplýsingar.

Vinsamlegast færðu 3650,00 € (EUR) yfir í eftirfarandi upplýsingar um bankareikning.

BANKUR: SE BANKEN (SEB)
NAME: PETER XXXXX
IBAN: SE8750000000XXXXXXXXXX
SWIFT / BIC: ESSESESS
Greiðslugerð: tafarlaus greiðsla (SEPA Transfer)

Vinsamlegast sendu afrit af staðfestingunni á flutningi pencilpenfed@gmail.com eftir greiðslu.

Jóhann

From: GísliXXXXXXXXXX
Sent: 20. september 2019 20:34
To: johannXXXXXXXXXX
Subject: Re: Brýnt verkefni

Já,

en fyrir hvað?

Gísli

From: johannXXXXXXXXXX
Sent: 20. september 2019 18:20
To: GísliXXXXXXXXXX
Subject: Brýnt verkefni

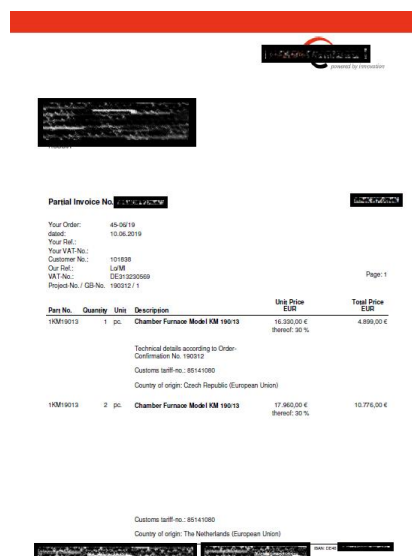
Gísli,

Er hægt að flytja 3650,00 € greiðslu í dag?

Jóhann

Algengt er að slík sé sent út á föstudögum til að gefa glæpamönnunum helgina til að koma peningum undan. Til eru hástig og lástig. Dæmið að ofan er lágstig, þar er pósturinn sendur úr öðru netfangi en með smá forritun er hann látinn líta út fyrir að vera frá réttum sendanda.

Hástig er þegar glæpamennirnir hafa komið sér inn í samskipti tveggja aðila og breyta síðan kvittunum til að greiðsla fari til þeirra í stað þess að berast réttum viðtakanda.



Dæmi um viðskipti sem eiga sér grundvöll en svindlurinum hefur tekist að komast inn í samskiptin og breyta reikningum til að fá greiðsluna á rangan stað. Reikningurinn er að öðru leiti alveg réttur í uppsetningu og útliti enda hafa þeir aðeins breytt honum.

Svindlararnir komast í skrár þar sem fram koma netföng formanna, forstjóra, framkvæmdarstjóra og gjaldkera. Slíkar upplýsingar liggja oft á lausu.

Fyrir nokkru var herjað á íþróttafélög en okkur hafa núna borist tilkynningar frá fyrirtækjum og foreldrafélögum. Það eru ekki mörg frjáls félagasamtök eða íþróttafélög sem mega við að missa 3.650 EUR / 513.000 ISK eða meira á þennan hátt en oft eru stjórnmenn og gjaldkerar í

sjálfboðavinnu og gera sér ekki alltaf grein fyrir hættunni. Dæmi eru um að fyrirtæki hafi tapað yfir hundrað milljónum og það hefur áhrif á allan rekstur. Heildartjón slíkra netglæpa síðustu tólf mánuði er komið yfir milljarð.

Góðar venjur

- Ef þú færð tölvupóst þar sem þú átt að greiða inn á áður óþekktan reikning þá skaltu hafa samband beint við aðilann sem sendi þér póstinn, helst með að hringja í viðkomandi eða með öðrum hætti. Oft er villandi texti settur inn í skeytin eins og „ég er á fundi og það er ekki hægt að ná í mig í síma“ en það er bara til að setja pressu á þann sem á að svindla á.
- Ekki ýta á reply, sendu frekar nýjan póst á viðkomandi. Þessi póstur er oft þannig frágenginn að reply fer á svindlarann en nýr póstur fer á réttan viðtakanda eða að báðir möguleikar koma upp og þá er oft augljóst að önnur er fölsk slóð.
- Ef þú ert í samskiptum við erlent fyrirtæki sem vill breyta greiðslufyrirkomulagi þá er líka full ástæða að hafa varan á sér og setja sig í beint samband við sína tengla þar. Sá sem greiðir inn á svindl er sá sem tapar og áhætta þeirra er því mikil.
- Hafðu varan á og ef þér finnst eitthvað tortryggilegt þá skaltu leita eftir staðfestingu.

Við hjá lögreglunni viljum heyra af slíkum tilvikum, sendið okkur póst á abendingar@lrh.is eða cybercrime@lrh.is með upplýsingum eða fyrirspurn.