Sosiale implikasies-‘sub-scenario’

Inligtings- en kommunikasietegnologie (IKT) gaan nie net oor hardeware- en sagtewarekwessies nie, maar ook oor kwessies soos die samelewing, wetlike, etiese, sekuriteits- en omgewingsaspekte.

1. Sibu het die volgende e-pos ontvang, wat blykbaar deur ’n amptenaar by Empire Bank gestuur is. Bestudeer die e-pos noukeurig en beantwoord die vrae wat volg:

> **From:** Empire Bank [mailto:john@empirebank.co.za]
> **Sent:** 17 May 02:38 PM
> **To:** Sibu_100@gmail.com
> **Subject:** Empire Bank Verifikasie - Sibu_100@gmail.com
>
> Beste gewaardeerde Empire Bank Lid,
>
> Hierdie e-pos is deur Empire Bank gestuur om jou e-pos adres te verifieer. Jy moet hierdie prosess voltooooi deur op die onderstaande skakel ke kluk en jou Empire Bank se wagwoord in die spasie in te tikk.
>
> Hierdie is vir jou eie beskerming, omdat sommige van ons lede nie meer toegang tot hul e-pos adresses het nie en ons dit moet nagaan. Om jou e-pos adres te verifieeer en toegank tot jou bankrekenaing te kry, klik op die onderstaande skakel:
>
> Klik hier om jou data by te werk

1.1 Wat is die algemene naam vir hierdie tipe slenter?

1.1 Uitvissingsbedrog / *Phishing.*

1.2 Daar is ’n hiperskakel onderaan die e-pos.

1.2.1 Verduidelik kortliks wat ’n hiperskakel is.

1.2.1 ’n Hiperskakel word in elektroniese dokumente soos e-posse en webblaaie gebruik. Dit is ’n ingeboude skakel en as jy op ’n hiperskakel klik, neem dit jou na ’n ander plek binne in die huidige dokument, of na ’n ander dokument op ’n ander plek – dikwels ’n webblad.

1.2.2 Moet Sibu op die skakel klik? Motiveer jou antwoord deur te verduidelik wat sal gebeur indien sy daarop klik.

1.2.2 Nee, Sibu moenie op die skakel klik nie. As sy daarop klik, sal sy heel moontlik na ’n webblad gestuur word wat ’n replika van die bank se webblad is, waar sy gevra sal word om aan te teken en so persoonlike en vertroulike inligting, soos PIN-nommers en wagwoorde, te gee.

1.3 Wat is die generiese of algemene naam van hierdie tegniek, waar mense oorreed word om inligting/toegang te gee, deur iemand wat maak of hulle die reg het om hierdie inligting te bekom?

1.3 *Social engineering* of sosiale manipulasie.

1.4 Wat word die proses genoem waar ’n e-pos-*header* verander word, sodat dit lyk of die e-pos van ’n ander persoon afkomstig is?

1.4 *Spoofing.*

1.5 Dit is altyd beter om self die URL van ’n webwerf, soos dié van jou bank, in jou webblaaier in te tik, as om op ’n skakel te klik. Sal dit help om dit te doen as jou rekenaar deur ’n *pharming*-aanval geaffekteer word?

Verduidelik jou antwoord deur kortliks te verduidelik wat *pharming* is.

1.5 Nee, *pharming* is ’n tegniek waar sekere aanpassings op die rekenaar gemaak is sodat, al tik die gebruiker die korrekte URL in, die gebruiker steeds na ’n ander webwerf herlei sal word, wat gewoonlik ’n replika van die ‘regte’ een is.

1.6 Mary sien dat daar baie teen *ransomware* gewaarsku word. Verduidelik wat *ransomware* is.

1.6 *Ransomware* is kwaadwillige sagteware wat data enkripteer (en veroorsaak dat jy dit nie kan gebruik nie) totdat jy ’n losprys aan die *hacker* betaal (dikwels deur Bitcoin te gebruik).

2. ’n Lid van die instansie wil seker maak dat Mary al die nodige voorsorgmaatreëls tref as sy met e-bankdienste besig is. Hy het ’n dokument hieroor van die bank se webwerf afgelaai.

2.1 Banke stel hul kliënte gerus deur ’n aantal sekuriteitsmaatreëls beskikbaar te stel om aanlyn bankdienste so veilig moontlik te maak.

Noem twee sulke maatreëls, buiten enkripsie (https).

2.1 Enige twee van die volgende:

- Aantekenwagwoorde/PIN-kodes.
- ‘Eenmalige wagwoorde’ vir elke e-banksessie, wat aan ’n selfoon of e-posadres gestuur word.
- Staking van die e-banksessie as dit vir ’n sekere tyd lank onaktief is.
- Boodskappe na die gebruiker se selfoon toe, wat die gebruiker laat weet dat ’n e-banksessie begin is, ens.

2.2 ’n Belangrike punt wat die bank uitlig, is dat dit gevaarlik is om e-bankdienste in ’n publieke plek, soos ’n kuberkafee, te gebruik, as gevolg van die gevare van *spyware* en *keyloggers*.

2.2.1 Wat is *spyware*? Verduidelik jou antwoord deur na ’n *keylogger* (en hoe dit werk) te verwys.

2.2.1 *Spyware* is sagteware wat jou rekenaar monitor en probeer vasstel vir watter doeleindes jy jou rekenaar gebruik. Dit stuur die inligting aan derde partye, sonder jou toestemming of sonder dat jy daarvan bewus is. ’n *Keylogger* is ’n program (’n soort *spyware*) wat die sleutels wat jy druk vaslê (en moontlik ook die bewegings van die muis). Dit kan ook skermkopieë maak, alles om gebruikername, wagwoorde, ens. in die hande te kry.

2.2.2 Gee twee redes hoekom anti-*spyware* gereeld bygewerk of opgedateer moet word, deur kortliks te verduidelik hoe anti-*spyware* werk.

2.2.2 Anti-*spyware* spoor *spyware* op wat op ’n rekenaar geïnstalleer is. Anti-*spyware* moet bygewerk word, sodat nuwer vorme van *spyware* opgespoor kan word. Anti-*spyware* hou ook databasisse in stand van webwerwe wat *spyware* versprei. Die databasisse word bygewerk wanneer die anti-*spyware* bygewerk word.

3. Vuyani gebruik ’n rekenaar wat nie aan die internet gekoppel is nie. Hy kan nie verstaan hoekom hy ’n virus op die rekenaar het nie, aangesien hy ’n antivirusprogram geïnstalleer het en nie aan die internet gekoppel is nie. Hy is ook seker dat hy nie ’n skadelike program soos ’n Trojaan op die rekenaar het nie.

   3.1 Verduidelik wat ’n rekenaarvirus is deur na twee doelwitte van ’n rekenaarvirus in jou antwoord te verwys.

   3.1 ’n Rekenaarvirus is ’n skadelike tipe program wat geskryf is om die normale werking van iemand se rekenaar te belemmer, sonder die persoon se toestemming of medewete. Dit kan ’n rekenaar in ’n *bot* verander (die rekenaar kan dan oor ’n afstand, via die internet beheer word) om skadelike sagteware te versprei of om ’n sekuriteitsgaping vir ’n ander program te skep. ’n Versameling van hierdie *bots* word ’n *botnet* genoem.

   3.2 Wat is ’n Trojaan?

   3.2 ’n Trojaan is skadelike sagteware wat homself voordoen as ’n nuttige toepassing. Dit kan gebruik word om ander skadelike sagteware op ’n rekenaar te installeer.

   3.3 Gee drie tipiese simptome van ’n rekenaarvirus.

   3.3 Enige drie van:
   - Vermindering in beskikbare skyfspasie
   - Skielik (onverwagte) stadige werking van ’n rekenaar
   - Antivirusprogram wat rapporteer dat ’n virus gevind is
   - Programme wat verdwyn/verander/nie meer werk nie, ens.

   3.4 Gee twee moontlike redes waarom Vuyani ’n rekenaarvirus het, ten spyte van die voorsorgmaatreëls wat hy getref het.

   3.4 Die antivirusprogram (virusdefinisies) is dalk nie op datum nie en hy het moontlik geïnfekteerde draagbare media, soos ’n *flash*-skyf, gebruik.

4. Een van die lede van die instansie het voorgestel dat ’n beleid vir aanvaarbare gebruik (*acceptable usage policy*) vir die gebruik van rekenaars by die sentrum opgestel word, en dat ’n plakkaat gemaak word om sake rondom netiket te beklemtoon.

   4.1 Waarna verwys *netiket*?

   4.1 Netiket verwys na beleefdheid teenoor ander gebruikers wanneer jy aanlyn is of elektronies kommunikeer.

   4.2 Gee vier netiketreëls wat op e-pos betrekking het en wat op die plakkaat aangebring kan word.

   4.2 Enige drie van:
   - Gaan spelling van boodskappe na voordat jy dit stuur.
   - Wees beleefd en op die punt af.
   - Moenie skinder of stories aandra nie.
   - Vermy groot aanhegsels.
   - Moenie kettingbriewe of *hoaxes* aanstuur nie.
   - Moenie in hoofletters tik nie, ens.

   4.3 Behalwe kwessies rakende netiket, noem nog drie sake wat in die beleid vir aanvaarbare gebruik aangebring moet word.

4.3 Enige drie van die volgende:

- Respekteer die privaatheid/data/intellektuele eiendom van ander.
- Moenie materiaal wat aanstoot kan gee, stoor of oopmaak nie.
- Moenie met sagtewareinstellings of hardeware peuter nie.
- Rapporteer enige probleme aan ’n personeellid.
- Jy mag nie sagteware installeer of verwyder nie.
- Waar en wanneer draagbare stoortoestelle soos *flash*-skywe en draagbare media-spelers gebruik mag word.

5. Baie van die jongmense in die plaaslike gemeenskap gebruik sosiale netwerktuistes soos Facebook, en dit blyk dat baie min van hulle weet hoe om die privaatheidsinstellings op te stel.

Hoekom is dit so belangrik om die privaatheidsinstellings op ’n sosiale netwerktuiste soos Facebook op te stel?

5. Privaatheidsinstellings laat toe dat jy kan spesifiseer wie jou inligting mag sien en wie nie – dit sluit foto’s en boodskappe in. Mens kan ook kies wie boodskappe op jou muur mag skryf.

6. Iemand het die trust gekontak vir ’n moontlike borgskap. Hulle wil egter seker maak dat die trust verbind is tot ‘groen rekenaarverwerking’ voordat hulle ’n borgskap oorweeg.

6.1 Verduidelik kortliks waarna *groen rekenaarverwerking* gewoonlik verwys.

6.1 Groen rekenaarverwerking verwys daarna dat mens die impak op die omgewing in gedagte hou wanneer jy (rekenaar-)tegnologie gebruik.

6.2 Een van die maniere waarop die trust geld kan spaar en ’n bydrae tot groen rekenaarverwerking kan maak, is deur die hoeveelheid papier wat vir drukwerk gebruik word, te verminder.

Gee twee maniere hoe dit gedoen kan word.

6.2 Enige twee van:

- Moedig personeel/gebruikers aan om die elektroniese weergawe van ’n dokument eers te proeflees voordat dit gedruk word.
- Maak meer gebruik van e-kommunikasie (e-pos) in plaas van drukstukke om dokumente te versprei.
- Druk dokumente dupleks/langs mekaar uit, ens.

6.3 Nog ’n manier waarby die trust tot groen rekenaarverwerking kan bydra, is om minder krag te gebruik.

Gee twee praktiese maniere waarop hulle minder krag kan gebruik.

6.3 Enige twee van die volgende:

- Gebruik energiebesparende toerusting/hardeware.
- Gebruik instellings op rekenaars om krag te spaar/hiberneermodus.
- Skakel toerusting wat nie gebruik word nie, af.

7. Een van die belangrikste voordele vir kursusgangers wat hul IKT-vaardighede verbeter het, is dat hulle in ’n beter posisie sal wees om ’n loopbaan te volg waar hulle moontlik sal moet ‘telecommute’.

   Verduidelik kortliks die konsep van *‘telecommuting’* of telependel.

7. In plaas van fisies na ’n tradisionele kantoor te reis om daar te gaan werk, kommunikeer werkers elektronies met mekaar (hul kliënte / werkgewers / klante).

8. Een van die rekenaars het ’n braille-sleutelbord en ’n ander een ’n *groot trackball* in plaas van ’n ‘normale’ muis.

   Aan watter gestremdhede sou ’n persoon waarskynlik ly as hy/sy ’n *braille-sleutelbord* gebruik of as hy/sy ’n *groot trackball* gebruik?

8. Braille-sleutelbord: gesigsgebrek, blindheid

   Groot *trackball*: gebrekkige motoriese beheer (verlamming, artritis, ens.)

9. ’n UPS moet op die bediener geïnstalleer word.

   9.1 Wat is die funksie van ’n UPS?

   9.1 Om die rekenaar / bediener teen elektrisiteitsprobleme te beskerm (bv. stuwinge, pieke, kragonderbrekings)

   9.2 Hoekom is dit belangriker om ’n UPS op ’n bediener as op ’n kliëntrekenaar te installeer?

   9.2 ’n Bedienerrekenaar bied bronne en dienste aan (baie) ander rekenaars op die netwerk. Daar is dus verreikende / negatiewe / duur gevolge as ’n bediener deur kragprobleme beskadig word, teenoor minder skade as ’n kliëntrekenaar beskadig word.

   Dit gee ook tyd om die bediener behoorlik af te sluit as daar ’n kragonderbreking is, om verlies van data te voorkom.

10. Die Trust bevorder Kickstarter – ’n aanlyn platform wat deur mense gebruik word om hul kreatiewe sake-idees te befonds.

    10.1 Gee twee voordele van die gebruik van ’n platform soos Kickstarter om ’n sake-idee te finansier.

    10.1 Enige twee van die volgende:
    - Om te bepaal of daar behoefte en ondersteuning vir ’n idee of produk is voordat jy tyd, moeite en geld daarin belê om dit te skep
    - Die eerste vrystelling van die produkte is alreeds ‘verkoop’ voor dit geskep is
    - Groter kans van befondsing deur veelvuldige donateurs (in plaas van op tradisionele leningsinstansies soos banke te vertrou)

    10.2 Gee een tipiese voordeel wat ’n persoon sou kon verwag om te ontvang, as hy/sy bygedra het, of geld belowe het (‘pledging’) tot ’n sake-idee wat dan wel geslaag het.

    10.2 ’n Beloning van een of ander aard (dikwels in ooreenstemming met die hoeveelheid geld belowe), soos die volgende:
    - Voltooide produk teen ’n laer prys
    - Spesiale toevoegings en aanpassings tot die produk wat nie beskikbaar sal wees vir mense wat nie geld belowe het nie, ens.

11. Gee een rede hoekom dit dalk nie ’n goeie idee mag wees om die rekenaars aan ’n *grid computing*-projek te laat deelneem nie, selfs al sou daar ’n vinnige internetkonneksie wees.

11. Enige een van die volgende:
    - Rekenaars mag stadiger werk
    - Moontlikheid van *malware*-infeksies
    - Risiko van rekenaarskade deur oorverhitting