Rämpspost (Spam)

Me kõik oleme leidnud oma postkastist soovimatuid reklaamkirju ehk rämpsposti ning nii mõnigi meist on hädas olnud sellega, et rämpsposti maht ületab soovitud kirjade mahu. Tartu Ülikooli kirjakaste kaitseb rämpsposti eest filtrite süsteem, mis peatab suurema osa rämpspostist enne, kui see jõuab meie postkastidesse. Paraku on rämpsposti saatjad sellega kursis ning leiavad pidevalt uusi viise, kuidas sellistest filtritest mööda saada, mille tõttu leiab mõni neist kirjadest ka tee meie postkastidesse.

Käesolev juhend annab vastused järgmistele küsimustele:

1. Kuidas rämpsposti ära tunda?
2. Mida rämpspostiga ette võtta?

Kuidas rämpsposti ära tunda?

Rämpsposti eesmärgiks on eelkõige teenida raha reklaami edastamisega, arvutikasutaja kontode (e-post, sotsiaalmeedia jne või isegi arvuti/nutitelefoni üle võtmine. Tegemist on internetipettuse ühe vormiga, mis põhineb identiteedivargusel ning saab reeglina alguse e-posti teel saadetud petukirjast.

Rämpspostile viitavad tavaliselt järgmised tunnused:

1. Imelik meiliaadress;
2. kahtlane pealkiri;
3. sisu imelik toon, grammatiliselt väär sõnakasutus.

Näide 1 - viiruste levitamine ja lunarahanõue:

Every once in a while we discover unwanted e-mails in our inbox, that sometimes make up most of the received e-mails. These are adverts or spam. The University of Tartu e-mails are protected by a series of filters, which prevent most of the spam from ever reaching a users inbox. Unfortunately, the people responsible for sending out spam are figuring out new ways to bypass these filters, which means that some spam e-mails will still end up in your inbox.

These instructions will answer the following questions:

1. How to identify spam e-mails?
2. What to do with spam e-mails?

How to identify spam e-mails?

Spam usually reaches us in the form of phishing, which is fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter personal information at a fake website, the look and feel of which are identical to the legitimate site, the only difference being the URL of the website in concern.

A phishing e-mail can be usually identified by the following symptoms:

1. The e-mail is sent from a public or strange e-mail address;
2. poor spelling and grammar;
3. The creation of a sense of urgency.

Example 1

```
From: Jossie Dick (AAA)<Jossie.Dick@colvilletribes.com>
Sent: 7. august 2018. a. 10:45
Subject: TÄHELEPANU WEB PASSWORD TOIMIB TÄNA

Teie OUTLOOK WEB-võrgu konto parool aegub täna.

Parooli muutmiseks järgige allolevaid juhiseid.
Külastage veebilehte OUTLOOK WEB Digital Intranet [!!!TEKST ON LINK MILLELE
EI TOHI VAJUTADA!!!].

Võrgussüsteemid
Juurdepääs piirkonna lauaarvutitele (nt. Kaugjuhtimispuldid-V :, W :, U :,
T: jne)
VPN-i juurdepääs väljaspool piirkonda
Traadita võrk või Interneti-ühendus sülearvutitelt või tahvelarvutidelt
E-post Outlooki, Outlooki veebi ja nutitelefonide kaudu
Adobe Connect
Rikastada
Online tööhõive taotlemise süsteem
Toitumisalased teenused MCS ja PCS
Oracle

Kui teil on küsimusi, võtke palun ühendust laienduse 7892 lehelt OUTLOOK WEB.

Aitäh,
Infoteenuste osakond
```

Ülaltoodud kirjas esinevad kõik rämpspostile viitavad tunnused.
Esiteks on kirja saatjaks keegi Jossie Dick, kes ei oma mitte mingit seost Tartu Ülikooliga. Kahtluse korral tuleks kontrollida välisveebist või siseveebist, kellega on tegu - kui isikut töötajate nimekirjas pole, on tegemist petukirjaga.
Teiseks on kirjal kahtlane pealkiri, mille keelekasutus on imelik ning ei viita ühelegi konkreetsele ülikooli infotehnoloogia teenusele. Infotehnoloogia osakond korraldab küll paroolivahetuskampaaniaid, kuid sellest teavitatakse listide ja kindlasti ka siseveebi vahenudsel.
Kolmandaks on kirja sisul imelik toon ja veider sõnakasutus. Kirja sisus leidub küll teenuste nimetusi, mida ülikoolis kasutatakse, kuid tervikpilt jätab siiski kahtlase mulje (nt "Rikastada" või "Toitumisalased teenused MCS ja PCS").

Näide 2 - viiruste levitamine (nt krüptoviirus):

```
From: Jossie Dick (AAA)<Jossie.Dick@colvilletribes.com>
Sent: 7. august 2018. a. 10:45
Subject: ITS HELP DESK

The IT Dept. will be performing repairs to integrate computer and phone mail
system tongiht starting at 9pm.
Therefore all staff are to CLICK HERE [!!!A LINK THAT YOU SHOULD NEVER CLICK
ON!!!] and enroll for the upgrrade.

Filling the submission form will enable us to migrate your account fully
into the system. Cyber Security is every one concern.




Thank you for the understanding...



ITS HELP DESK/SUPPORT
(C) Copyright 2018 Microsoft
All Rights Reserved
```

The example above has all the symptoms of a spam/phishing e-mail.
First of all, the sender is someone called Jopssie Dick, who is in no way connected to the University of Tartu. When in doubt, check the intranet's or the public website's employee search function - if the person is not listed, the message is fraudulent.
Secondly, the e-mail's subject is strange and it doesn't look or sound like anything the university's IT-office would send out. IT-office will send out messages for upgrades every once in a while and that information will always be added to the intranet as well. Please remember, that we will never ask for your username and password!
Lastly, the e-mail creates a sense of urgency and has poor spelling and grammar. This is a clear sign of a phishing e-mail.

Example 2

```
Label: 25343391367031008
Saatja: post@usps.com
Saaja:        XXX

invoice.zip

The courier company was not able to deliver your parcel by your address.

Cause: Error in shipping address.
Label: 31585036553374581

Print this label to get this package at our post office.
Please attention!
For mode details and shipping label please see the attached file.
Please do not reply to this e-mail, it is an unmonitored mailbox!

Thank you,
USPS Logistics Services.

CONFIDENTIALITY NOTICE:
This electronic mail transmission and any attached files contain information
intended for the exclusive use of the individual
or entity to whom it is addressed and may contain information belonging to
the sender UPS , Inc. that is proprietary,
privileged, confidential and/or protected from disclosure under applicable
law. If you are not the intended recipient, you
are hereby notified that any viewing, copying, disclosure or distributions
of this electronic message are violations of
federal law. Please notify the sender of any unintended recipients and
delete the original message without making any copies.
Thank You
```

Ülaltoodud kirjas on olemas kõik rämspostile viitavad tunnused, mis said mainitud eelmise näite juures. Erinevuseks on see, et kirjale on lisatud manus nimega **invoice.zip**. Mitte ükski organisatsioon ei saada ametlikke dokumente ***.zip** formaadis, kuna see ei ole turvaline ning viitab koheselt petukirjale. Sellised dokumendid edastatakse ***.pdf** formaadis. Juhul, kui tegemist on millegi muuga, siis tuleks kindlasti olla äärmiselt ettevaatlik!

Ülaltoodud selgituste põhjal tuleks rämsposti tuvastamiseks küsida endalt:

1. Kas ma tunnen kirja saatjat? Kas kiri on tulnud ametlikut @ut.ee aadressilt või mõne muu tuntud organisatsiooni aadressilt? Kas ma saan seda kontrollida?
2. Kas ma ootasin sellelt saatjalt kirja?
3. Kas kirjaga on kaasas manus, mille failitüüp on mulle teada (nt *.pdf, *.docx, *.doc, *xls, *xlsx)?
4. Kas kirja pealkiri on ametlik ja korrektselt sõnastatud?
5. Kas kirja sisu on kuidagigi seotud minu tööga või organisatsiooniga?
6. Kas kirja sisu on ametlik ja korrektselt sõnastatud?

Kui vastasite ühele neist küsimustest sõnaga "ei", siis tuleks olla äärmiselt ettevaatlik!


```
Label: 25343391367031008
Saatja: post@usps.com
Saaja:        XXX

invoice.zip

The courier company was not able to deliver your parcel by your address.

Cause: Error in shipping address.
Label: 31585036553374581

Print this label to get this package at our post office.
Please attention!
For mode details and shipping label please see the attached file.
Please do not reply to this e-mail, it is an unmonitored mailbox!

Thank you,
USPS Logistics Services.

CONFIDENTIALITY NOTICE:
This electronic mail transmission and any attached files contain information
intended for the exclusive use of the individual
or entity to whom it is addressed and may contain information belonging to
the sender UPS , Inc. that is proprietary,
privileged, confidential and/or protected from disclosure under applicable
law. If you are not the intended recipient, you
are hereby notified that any viewing, copying, disclosure or distributions
of this electronic message are violations of
federal law. Please notify the sender of any unintended recipients and
delete the original message without making any copies.
Thank You
```


This has all the symptoms of a spam/phishing e-mail, which will encrypt your files and then try to ransom them. The main difference is that there is no link in the e-mail, but an attachment called **invoice.zip**. No modern organization sends out official documents in a ***.zip** container, since that is considered unsafe and telltale sign of a phishing e-mail. Invoices and documents are almost exclusively sent out in the ***.pdf** format.

If it is anything else, you need to be extra careful!

To summarize, you need to ask yourself the following questions in order to identify spam or phishing:

1. Do I know the sender? Was the message sent from an official e-mail address (@ut.ee)? Can I verify the sender's e-mail address?
2. Was I expecting this e-mail?
3. Are the extensions of the files attached to the e-mail known to me (i.e .pdf, *.docx, *.doc, *xls, *xlsx)?
4. Is the e-mail's subject official and uses correct spelling and grammar?
5. Is the content of the e-mail related to my work or my organization?
6. Does the content of the e-mail use correct spelling and grammar?

If the answer to any of the questions above "NO", then you should be extra careful!

Rämsposti ja erinevate petukirjade tüüpide kohta saab täiendavalt lugeda siit: https://et.wikipedia.org/wiki/Internetipettus

Mida rämpspostiga ette võtta?

Kuna rämpsposti levitajad otsivad pidevalt uusi võimalusi organisatsioonide rämpspostifiltritest mööda pääsemiseks, ei ole kõiki kirju võimalik blokeerida enne, kui need on juba meie postkasti jõudnud.

Rämpsposti tuvastamisel tuleks see kustutada ning selles asuvaid viiteid või manuseid mitte avada! Kui tekib kahtlus, kas tegemist on rämpspostiga, tuleks kindlasti nõu küsida Tartu Ülikooli Arvutiabilt.

More info on spam and e-mail fraud: https://en.wikipedia.org/wiki/Email_fraud

What to do with spam e-mails?

Since spammers find ways to bypass the e-mail filters set up by the e-mail administrators, it is not possible to block all of them, before they reach your inbox.

When receiving spam or phishing e-mails, just delete them and never open any of the included links or attachments.

When in doubt, contact the University of Tartu Helpdesk.