

### **Task 1: Can you... scam me**

**How you might be able to verify, whether the message is coming from the claimed entity.**

Email Verification Example -

Scenario: Receive an email purportedly from the bank requesting sensitive information or urging to click on a link to verify account details.

- Check the Sender's Email Address
- Inspect Email Content
- Hover Over Links
- Contact Your Bank

### **1A) Email and URL phishing**

**What methods have been used on the message to convince the user to make an action and how the information is likely obtained?**

The phishing email employs several tactics to convince the recipient to take action,

Urgency: Email elicits sense of urgency by claiming unusual bank account activity and temporary suspension of online banking access, prompting users to act without verifying message's authenticity.

Threat of Consequences: The email warns of a 24-hour account suspension, urging recipients to click the provided link to avoid further damage.

Impersonation: Attackers impersonate S-Pankki Finland using a spoofed email address to increase the likelihood of recipient compliance with a request.

Phishing email may have obtained recipient's name & email address through various mean including,

Previous data breaches: Cybercriminals frequently obtain personal information from previous data breaches involving financial institutions or other organizations.

Phishing campaigns: The attackers may have previously launched phishing campaigns to obtain personal information, including email addresses.

Publicly available information: Email addresses can be obtained from publicly available sources like social media profiles or online directories.

Phishing emails use social engineering to trick recipients into clicking on a link to a fraudulent website, revealing sensitive account information.

**Who owns the domain spanki.fi related to the previous message? How about the domains s-panki.fi or spankki.fi?**

spanki.fi

Domain is spanki.fi and Registrar is Finnish Communications Regulatory Authority

s-panki.fi and spankki.fi

These domains are registered due to typosquatting. Typosquatting is the practice of registering domain names that resemble legitimate ones, with the aim of exploiting user typos. Ownership of these domains can be challenging to determine without conducting a WHOIS

**Is anyone capable to register free domain names, even similar to known brands? Take a brief look for registration requirements and process for .fi domains. Think about new registrations of S-Pankki domains.**

Free domain names can be registered by anyone, but authorities have policies to prevent malicious use, such as trademark infringement or phishing, to prevent fraudulent activities.

.fi domains, the registration requirements and processes are governed by the Finnish Communications Regulatory Authority. To register a .fi domain, individuals or organizations typically need to provide certain information and adhere to FICORA's registration guidelines.

For new registrations of domains similar to known brands like "S-Pankki," there are several factors to consider:

Trademark Protection - Trademark owners can use legal methods to dispute or prevent similar domain names that could infringe on their trademark rights.

Anti-Phishing Measures - Domain registration authorities may implement policies to prevent phishing and fraudulent activities by conducting checks on the legitimacy of the registrant's identity and intentions.

Monitoring and Enforcement - Domain authorities and brand owners regularly monitor new domain registrations for suspicious activity and take action against malicious domains like phishing or trademark infringement.

**Why it is so important pay attention to exact URLs and why can we trust the URLs in the first hand? Only a short explanation about the trust is required.**

Exact URLs are crucial as they can indicate website legitimacy or message authenticity, and trust in URLs is essential for various reasons.

Phishing Prevention - Phishing scammers create fake websites to deceive users into disclosing sensitive information. Users can detect inconsistencies or abnormalities in the URL to prevent such attacks.

Security - Websites use secure protocols like HTTPS to encrypt data transmitted between the user's browser and the server, ensuring user interactions are secure and protected from eavesdropping or tampering.

Identity Verification - URLs reveal website owner's identity, matching branded domain names. Users can verify website authenticity by cross-referencing URLs with trusted sources like official websites or domain registration records.

**Look for the sender from the .eml message. How the message has been sent? You should be able to identify the service.**

Message was sent from a server with the hostname "emkei.cz" and the IP address 89.187.129.24. It appears that the email originated from a Postfix server running on emkei.cz.

Email was routed through Microsoft Outlook servers, suggesting the sender used an external service provider to obfuscate its origin. It was sent using a Postfix server on emkei.cz, indicating control or access. Sender's claimed identity and the sender email address are likely spoofed, as indicated by the lack of DKIM and SPF authentication in the email headers. This suggests that the email is likely part of a phishing attempt rather than a legitimate communication from S-Pankki Finland

**What headers are telling about DMARC, DKIM and SPF checks**

DMARC - Indicates that DMARC check failed. The DMARC policy for the sender domain spanki.fi specifies that no action should be taken on messages that fail the DMARC check. This means that the email authentication failure will not result in any specific action according to the DMARC policy.

DKIM - Indicates that DKIM check failed. The message was not signed with DKIM.

SPF - Indicates that SPF check failed. Sender domain spanki.fi doesn't designate permitted sender hosts.

**Now, do you think that these checks (especially the failure of them) will likely lead for previous mail to be deliver into spam rather than content on email server which has only SpamAssassin?**

Emails requesting sensitive information and claiming unusual account activity are likely to be flagged as spam by most email servers and filtering systems, including those with SpamAssassin. Suspicious Links, Urgency and Threats may be the caused to this. This email, likely marked as spam by spam filtering systems like SpamAssassin, is likely to be rejected. It's crucial to remain watchful and avoid clicking on suspicious links.

**If you attempt to spoof some of these domain owners, in which cases the messages are not delivered regardless of the content? (Who has configured their servers correctly (also with DKIM and SPF) with reject policy?)**

SPF helps prevent sender address forgery by verifying the sender's IP address against a list of authorized sending hosts for a domain. In this email, the SPF result indicates that the sender's IP address (89.187.129.24) is not authorized to send emails on behalf of the domain "spanki.fi". However, SPF alone does not enforce rejection; it merely provides a mechanism for validation.

DKIM adds a digital signature to email headers to verify that the email comes from an authorized source and has not been altered in transit. In this email, DKIM is not configured, meaning there is no DKIM signature present.

The domain owner of "spanki.fi" has not configured their servers correctly with a reject policy for SPF and DKIM. Therefore, spoofing attempts targeting this domain may still succeed, as the email system does not outright reject emails that fail SPF or DKIM checks.

### **1B) Combining knowledge**

**Will the message be delivered into the spam more likely because of the content rather than sending entity?**

Yes, the message is likely to be flagged as spam primarily because of its content rather than the sending entity. Following reasons to be caused to be,

Content Patterns - The email contains spam-like elements, including urgent requests for help, large sums of money, health-related references, and requests for personal information or financial assistance.

Phrasing and Language - The language used in emails, such as urgently needing trust and assistance, and promising compensation, is frequently used in spam messages to manipulate recipients into taking action.

Email Structure - The email follows a common scam pattern, presenting a personal story followed by a request for assistance and contact information for further communication.

The combination of these factors is likely to trigger spam filters, leading to the message being delivered into the spam or junk folder rather than the inbox.

**Identify at least five different psychological manipulation techniques what have been used in the message.**

Appeal to Emotion - The sender shares their cancer diagnosis and their desire to donate to charitable organizations, expressing sympathy and empathy to the recipient.

**Urgency** - The sender emphasizes the urgent need for assistance due to their health condition, implying time is running out, putting pressure on the recipient to respond quickly.

**Authority** - The sender, presenting themselves as a successful businesswoman, banker, and corporate executive, may gain trust and comply with the recipient's request due to their credibility and authority.

**Social Proof** - The sender uses social proof to justify their desire to donate money to charity, citing Jon Huntsman as an example of someone who has made significant charitable contributions.

**Reciprocity** - The sender compensates the recipient and their family for their assistance in distributing funds, demonstrating the principle of reciprocity and potentially making the recipient feel obligated to respond positively.

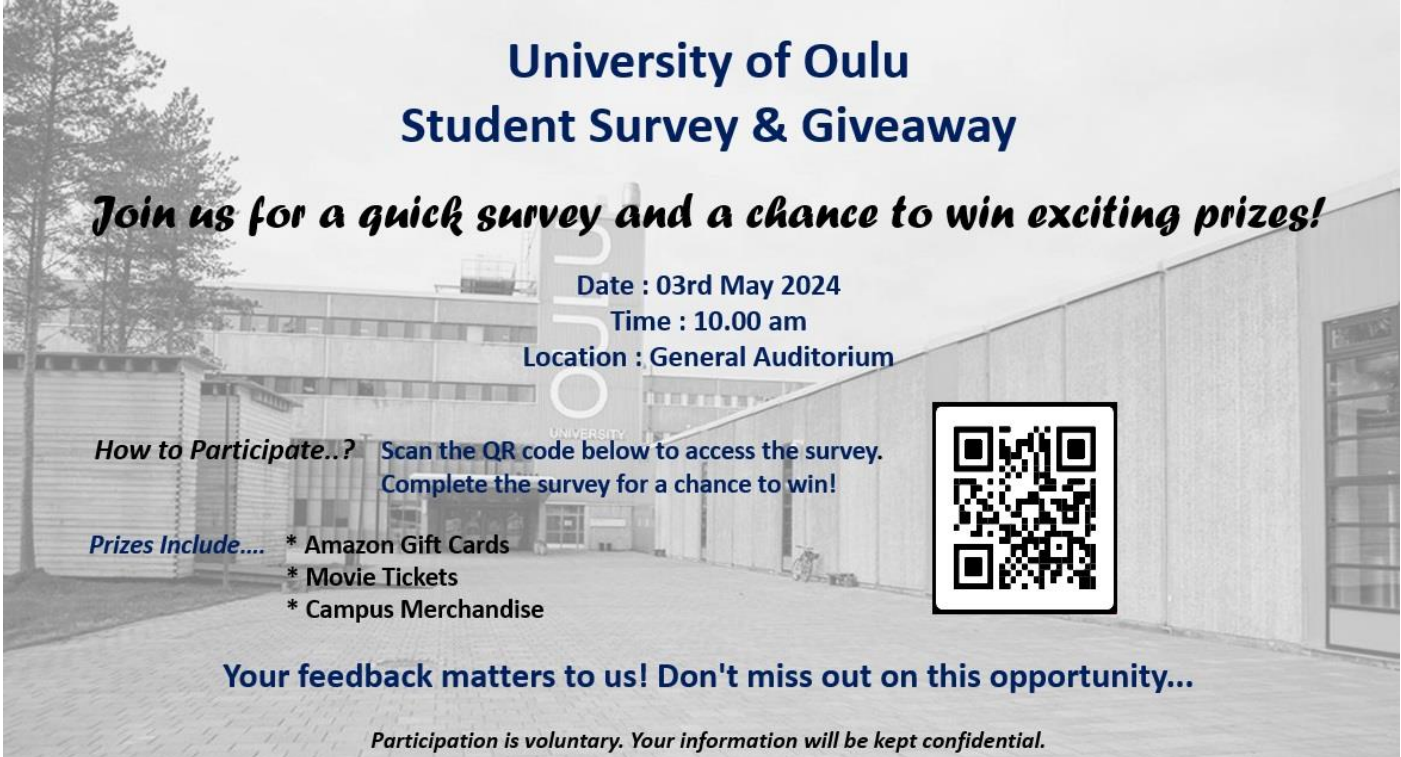
### 1C) Building a credential-stealing site

#### What was the purpose of 301 response code and location header?

The purpose of the 301 response code and the Location header is to redirect the user to the genuine Netflix website after capturing their credentials. This helps maintain the impression of validity while still allowing the attacker to produce sensitive information.

### Task 2: Social Engineering Toolkit

#### 2A) QR Code Credential Harvest - The poster with the QR code



**University of Oulu**  
**Student Survey & Giveaway**

*Join us for a quick survey and a chance to win exciting prizes!*

Date : 03rd May 2024  
Time : 10.00 am  
Location : General Auditorium

**How to Participate...?** Scan the QR code below to access the survey.  
Complete the survey for a chance to win!

**Prizes Include....**

- \* Amazon Gift Cards
- \* Movie Tickets
- \* Campus Merchandise

**Your feedback matters to us! Don't miss out on this opportunity...**

*Participation is voluntary. Your information will be kept confidential.*

**Scenario for usage. Explain in detail why your poster might be an effective way to collect credentials. Is it targeted to some specific group? Why it might work for them?**

**The site used for harvesting. You can test the QR with your phone and open the site in its browser.**

**Screenshot of the credential harvest tool successfully returning you the input credentials (Your name as username and surname as password)**

Scenario for Usage -

College campus scenario where students are preparing for final exams. During this stressful time, they are looking for convenient ways to access study materials and resources online. Our malicious actor takes advantage of this situation by creating a fake poster advertising a "Final Exam Study Guide Giveaway."

As students eagerly scan the QR code to access the supposed study guide, they unwittingly land on the malicious actor's credential harvesting page. The page, disguised as a login portal for accessing the study guide, prompts users to enter their university credentials. Once submitted, the credentials are harvested by the attacker for nefarious purposes. The poster leverages psychological tactics, targeted messaging, and perceived legitimacy to entice college students into scanning the QR code and falling victim to the credential harvesting scam.