- What does the "Not Secure" warning mean in the first picture and what risks does visiting sites with the warning pose?

  The “Not Secure” warning means there is a lack of security (SSL Certificate) for the connection to that page. Basically, it is to alert the user that information sent and received with that page is unprotected and it could potentially be stolen, read, or modified by attackers, hackers and other entities.

- Why does the second site show up as "trusted" to the browser?

  It means that the certificate for the second website is issued by a “trusted” Certificate Authority (CA), and the browser will establish a secure connection with the website. If the certificate is not issued by a trusted CA, the web browser will display a warning message and the user will be prompted to proceed with caution.

- What other ways are there to detect a phishing/scam site?

  There are multiple methods to detect a phishing/scam website.

  1. **Check the website’s URL and domain name.**

  Any suspicious variations or misspellings that could indicate a fake website. For example, “g00gle.com” instead of “google.com”.

  2. **Examine the website’s design and content**

  Phishing websites often mimic the design and layout of legitimate websites, but there may be subtle differences.

  3. **Be cautious of unsolicited emails or links.**

  If you received an email or message with a link to a website, exercise caution.

  4. **Use phishing website databases.**

  Several organizations maintain databases of known phishing websites.

  5. **Check online reputation.**

  Perform a search online to see if others have reported the website as suspicious or have had negative experiences with it.

  6. **Utilize browser extensions and security software**

  Install browser extensions or security software that can help detect and block known phishing websites.

- Are there any tools available online?

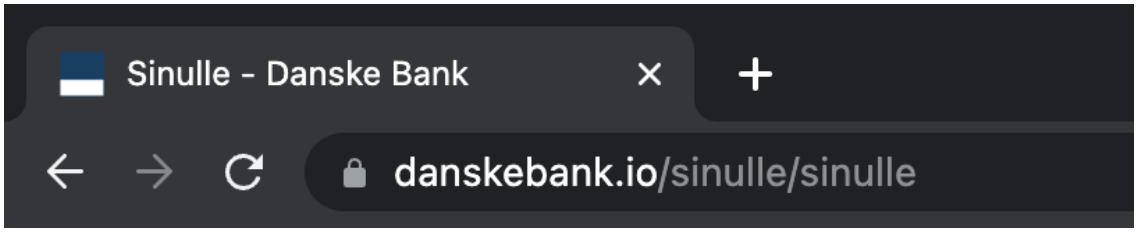
  Yes, there are several tools available online for phishing website detection.

- **VirusTotal:** It is a free online service that analyzes suspicious files and websites for malware and other threats.
- **PhishTank:** It is a community-driven database of phishing websites. Anyone can use to check the safety of a website.
- **Google Safe Browsing:** Google Safe Browsing is a service that helps protect users from malicious websites. It is built into Chrome and other popular web browsers.
- **Zscaler:** It is a cloud-based security platform that protects users from phishing attacks and other threats.
- **NoPhish:** This website offers a phishing protection service that can be used to protect businesses from phishing attacks. It uses a variety of methods to detect phishing websites, including machine learning and human analysis.
- **EasyDMARC:** This website offers a phishing link checker tool that can be used to check the safety of links in emails, text messages, and other online content.

- What is typosquatting and how does it relate to the pictures?

  Typosquatting is a type of cybercrime that involves registering domain names that are common misspellings of well-known websites. Hackers do this to lure unsuspecting visitors to alternative websites, typically for malicious purposes, such as:

- Stealing personal information, such as credit card numbers or passwords.
- Downloading malware to visitors' devices.
- Displaying malicious advertisements.
- Redirecting visitors to other malicious websites.



In this website address (Picture 2), **Typosquatting has been implemented by changing the domain name from danskebank.fi to danskebank.io**

- What is UDRP and how does it help with combatting typosquatting?

The Uniform Domain-Name Dispute-Resolution Policy (UDRP) is a policy adopted by the ICANN that provides a mechanism for the resolution of disputes over domain names. It is designed to be a quick and inexpensive way to resolve disputes involving domain names that have been registered in bad faith..

The UDRP can be used to combat typosquatting because it allows trademark owners to file a complaint against the registrant of a typosquatting domain name. If the complainant is successful, the domain name will be transferred to the complainant or canceled.

To be successful in a UDRP complaint, the complainant must prove the following three elements:

1. The domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights;
2. The registrant of the domain name has no rights or legitimate interests in respect of the domain name; and
3. The domain name has been registered and is being used in bad faith.

Typosquatting typically falls within the category of bad faith, as typosquatters typically register domain names with the intent to attract Internet users to their websites for commercial gain, by creating a likelihood of confusion with the complainant's trademark.

- If you were to own the domain ouspg.org and would be running your crypto banking application at bank.ouspg.org, what domains could you monitor for warning signs of possible phishing attempts against your customers?

I must monitor a variety of domains for warning signs of possible phishing attempts against my customers. Like,

- **Domains that are similar to bank.ouspg.org domain name.**

  For example, bank.ousbg.org, bank.ouspg.io, bank.osupg.org etc.

- **Domains that are associated with ouspg.org.**

  For example, crypto.ouspg.org, customer.ouspg.org, etc.