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

In the first picture. The browser shows. Not secure because the page is being loaded without any encryption like it is using plain HTTP or the TLS certificate might be invalid.

There are several risks involved if you proceed with such warning process, that include credential thefts (passwords, your Otps or other critical information) can be accessed if you are not connected to a secure website. And the other issue, could be related to tampering; any attacker on the network can change the page, or could inject some malware, or maybe change your credentials. There is also a possibility of a phishing attack where an attacker could pose a look-alike domain without any valid TLS certificate.

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

The second image shows a secure site or trusted site because the site is accessed using a secure hyper transfer text protocol (HTTPs) instead of simple HTTP.

**What other ways are there to detect a phishing/scam site? Are there any tools available online?**

There are different tools available to identify phishing/scam sites. Like, Google Safe Browsing or one can use VirusTotal website to scan the URL across many engines and validate its authenticity. There is also a possibility to perform certificate transparency search for suspicious look-alikes.

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

Typosquatting is a type of cyber-attack for phishing that uses registered domains look-alikes of the original domains but with misspellings or using some extra or missing letters. In the first picture we can see that the website being used (danskebankk.fi) has multiple Ks in it, which is a classic extra letter typo trick and in the second image we can see that (danskebank.io) is a top-level domain swap means it is not using the official Finnish domain (.fi) of the bank and these both are very common phishing tricks.

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

UDRP in (Uniform Domain Name Dispute Resolution Policy) is an ICANN process that lets trademark owners (for example Danske Bank, Apple) file a complaint to suspend domains registering in a bad faith that are similar to their official trademark. It is an administrative or civil remedy against cybersquatting which compliments takedown reports to registrars and hosting providers.

**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?**

If I were to own the said domain and run my crypto banking, I would watch out for Certificate Transparency for different domains or certificates containing ouspg or bank.ouspg or I would create a watch out list for top level domain swaps, various typos or words tricks. Also I would track phishing styles subdomain on other bases, (e.g. ausg.org.secure.com) or similar. When the hits appear, I would create such a system which checks the certificate details and move quickly with taking down host or if needed would take the action by invoking the UDRP.