Task 1

At first glance, these three websites look very similar. However, if you have knowledge about cybersecurity, you can see important differences. Some of these websites are very risky and dangerous, while only one of them is truly safe.

The first picture looks like the official Danske Bank website, which is a large Nordic bank. But if you look closer, you will notice something strange. The website address is different: there is a symbol that looks like a pyramid with an exclamation mark inside. The browser also shows the warning “Not secure.”

This means your information is vulnerable because the website does not use a valid SSL/TLS certificate. If you visit such a site on a public network (for example on a train or city Wi-Fi), anyone could intercept your information. If cybercriminals uses tools like Wireshark, they could easily capture your important details such as passwords, bank access, and even money.

The second picture looks like a secure site, but the address ends with “.io.” This is the country domain for the British Indian Ocean Territory. While some companies do use “.io,” in this case the website is not official or trusted. Information sent to it is still vulnerable and at risk.

The third picture shows the real and safe website. The address ends with “.fi” (Finland’s country domain). There is also a padlock symbol next to the address, which means the site uses HTTPS with a valid security certificate. Your information here is encrypted and protected, so criminals cannot easily steal it.

SSL systems changed after 2014. Before that, many security problems (such as the Heartbleed bug) allowed hackers to steal passwords, bank access, and other sensitive information. After this, the newer TLS and DTLS protocols were introduced to improve security.

Today, if you use a trusted website like in the third example, your information is safe because of encryption and modern network protocols.

There are a couple of important things could check:

First you could look the URL carefully, strange letters, symbols or numbers in the address may mean that the website is fake. Second you could look for HTTPS – ”http” means th esite is not secure, while ”HTTPS” means it is encrypted. Check also the padlock symbol. A closed padlock means the connection is secure.

Typosquatting you should be careful. Fake sites may look almos the same as famous ones. Like in the excam about danskebank. UDRP protection allows organizations to take action against fake or abusive websites. If a dispute arises UDRP can decide which website is real and the fake one will be removed.

By paying attention to small details in the address, HTTPS status and security, you can protect your personal information from phishing, typosquatting, and other online threats.