Aarni Ylitalo

2584582

Task 2

**Task 1A**

Browser in the picture looks like Chrome, which shows website as “secure” when they use HTTPS. “Non-secure” sites use regular HTTP which does not encrypt the request. That means sensitive details e.g. login information will be sent as plain text over the web.

Second site looks as trusted because it uses HTTPS, despite being quite obvious scam URL. There are some tools for example F-Secure offers service to check if site is good to go.

Typosquatting is when bad actors make a real looking website and have its URL look like real one with some spelling error or change top level domain like in the middle picture. Uniform Domain-Name Dispute-Resolution Policy (UDRP) is one way of combatting against typosquatting with the help of court.   
  
If I owned ouspg.org I would try to look for any subdomains that I have not made.

**Task 2**

Chip cards are more secure, because they have one time digital signature for each purchase. Magnetic stripe cards have static data which can be exploited.

EMV cerftificates are transaction authentication standards. For level 1 the responsibility belongs to hardware supplier, level 2 for software supplier and level 3 for merchants. For company to get certified they need to decide on terminals, payment gateway software and acquirers that process transactions. When those are chosen, company can apply for the two phase process to get the certification. With standardization payments via terminal come more secure.

Payment card data can get stolen from companies when shopping online, payment terminals can be tampered with a device that reads the data from the card without user knowing it and that data can be later used to create a copy of the card or be sold forward.

MFA can be used to put a code that comes in your banking app when logging in.

Its another layer of security which requires lot of effort to bypass.

I use google authenticator to login and my bank has 2FA.

2FA bypass attacks include social engineering, SIM-Jacking, man-in-the-middle attack etc…

**Task 3**

Evolution of card fraud

Card fraud is when someone uses another ones credit or debit card without their permission. There are multiple ways of how to steal someones card details. One can steal someones identity information and with that open account in a bank. After opening an account, the criminal can make purchases or withdrawal cash with the card. Criminals can also also use victims identity to takeover their account. This needs some more information about the victim that can be acquired by finding their mail trash which might include sensitive information. Other ways to get this data is by phising brute force attacks or one click apps. The United States is the most popular country for card frauds. The trend of card frauds has been going up due to people using more cards and much less cash. Also ever rising online shopping plays a major part in this. The EMV standards have been made and countries and EU laws are being made to make this trend go down. The revised Payment Services Directive (PSD2) is an attempt to unify payment services and make payments more secure. This enhances security and consumer data. PSD2 standards strong authentication and common and secure communication. In addition of previous transactions and devices are monitored for unusual transactions. Lastly it attempts to provide an standardized and reliable access interface for payment accounts. As stated before online transactions have been rising for a long time and are the highest risk of card data ending up in the wrong hands. Poor data management can lead to serious issues and unfortunately when data breaches happen card details or account information have been saved even as plain text. This makes breaching into companies servers a lucrative opportunity for criminals. Given this it should be made best effort to prevent data breaches. Tokenization can be one solution for this. In tokenization sensitive data is replaced with non-sensitive data. This is done by making the payment token a unique number string generated from PAN. They are made in real time and used by predefined domains or environments.