Research Document on security awareness

## Research Question

**What kind of topics does cyber security awareness encompass, and which of them will be in the game?**

I started by looking at the wikipedia page on cyber security awareness. A lot of online sources confirm what my stakeholder explained; there are many trainings out there, but they are targeted towards large companies and cost money.  
Source: <https://en.wikipedia.org/wiki/Internet_security_awareness>

There, I found a list of potential threats to cyber security:

**Threats**

**Threat agents** or threat actors are the perpetrators of the threat and usually look for the easiest way to gain access into a network, which is often the human element. However, these cyber threats can be mitigated. Some common threats include but are not limited to below.

**Social engineering** is when someone uses a compelling story, authority, or other means to convince someone to hand over sensitive information such as usernames and passwords. An end user with cyber security awareness will have the ability to recognize these types of attacks which improves their ability to avoid them.

**Phishing** is a form of social engineering. It is a popular attack that attempts to trick users into clicking a link within an email or on a website in hopes that they divulge sensitive information.  This attack generally relies on a bulk email approach and the low cost of sending phishing emails. Few targets are fooled, but so many are targeted that this is still a profitable vector.

**Spear phishing** is an email crafted and sent to a specific person to whom it may appear to be legitimate. It is a form of phishing, but it is more convincing and more likely to succeed than traditional phishing emails because it tailors the email to the victim.   Its deployment can range from a bulk automated process, such as accessing the address book of a past victim and sending simple phishing attacks to their contacts (thus appearing to come from a recognized past contact), to more sophisticatedly hand-written communications to target specific recipients.

**Vishing** or voice phishing is a form of social engineering that involves contacting individuals via traditional landlines, telephony (i.e., Voice over IP), automated text-to-speech systems, or other forms of voice communications to trick them into divulging sensitive information like credit card data.

**Smishing** or SMS phishing is social engineering that leverages SMS or text messages as the vector to trick end users into divulging sensitive information.

**Tailgating** is a physical security social engineering attack in which an unauthorized individual can access a location by following an authorized user into the location without the authorized user's knowledge.

**Piggybacking** is a physical security social engineering attack in which an unauthorized individual can access a location by following an authorized user into the location with the authorized user's knowledge.

**Malware** is software created and used for malicious intent.  It includes a range of software to include but is not limited to viruses, trojan horses, worms, rootkits, spyware, and crypto-jacking.

**Ransomware** is another cyber threat where attacks are carried out on the computer system but are often the result of a social engineering attack.  This type of malware encrypts data and holds it for ransom which could paralyze the whole computer system.

**Internet of Things** (IoT) based attacks are a form of cyber threat in the 21st century and beyond that leverage vulnerabilities in the embedded devices found in, i.e., cars, refrigerators, and smart speakers or digital assistants.

I also found a list of countermeasures that are taken or can be taken against these threats.

**Anti-Malware Protection:** Anti-malware is sometimes referred to as anti-virus**.** This type of application is used to protect systems against malicious software by preventing, detecting, and deleting the malware.  Some popular malware includes computer viruses, ransomware, rootkit, trojan horses, and worms.  Security end user awareness guidelines include device scans for malware and updating the anti-malware application definitions.

**Data Protection and Privacy:** There are various types of data that might be mandated to be protected from unauthorized disclosure, including personally identifiable information (PII), protected health information (PHI), intellectual property (IP), and other sensitive information. Security awareness guidelines include teaching related to data classification, encryption, data anonymization, and data masking or data obfuscation.  Permissions and who can access data, which includes file sharing via email attachments, are additional safeguards that could be discussed. Another data protection control that could be included is backing up data as it could be restored if the original becomes unavailable.

**Device Management:** involves knowing how to protect mobile devices and computers.  Device Management is also concerned with security related to Bring Your Own Device (BYOD).  Security awareness guidelines include encryption, protecting the system with a password, PIN, or multi-factor authentication, and other forms of credential.  Additional awareness tips include end-users downloading, installing, and reviewing applications and the requested permissions from unknown sources.  According to, another awareness tip is to read reviews and comments about the application before installing it.  Additionally, the use of public WIFI is another discussion point. Device management also relates to maintaining an accurate inventory of assets from purchase to disposition. This includes knowing when to wipe a device and media sanitization.

I**ncident Response:** An incident is any observable event of malicious intent.  Security awareness guidelines for end-users include what types of events are considered suspicious or malicious, who should be contacted if an incident occurs, and what actions should be taken in the event of an incident.

**Internet of Things Security:** are remotely controlled capable, resource constrained devices with embedded sensor chips that interact with people and objects to collect data and provide it to remote sources on the Internet for additional analysis in an effort to personalize and customize a user's experience. These devices include but are not limited to smart speakers, wearable devices like smart watch, surveillance cameras, lights, door locks, thermostats, appliances and cars.  Guidelines include maintaining an asset inventory, patch control, and changing default credentials.

**Password Management:** A password is a string of secret characters used to authenticate a user's account. Security awareness guidelines suggest presenting requirements for creating a strong password or Passphrase, how frequently passwords should be changed, and how to protect passwords. Additionally, guidelines suggest the need to change all default passwords and to not share passwords with others. Additional protection options could include making end-users aware of using multi-factor authentication, password managers, and awareness of various password-related threats like password cracking.

**Patching:** Software and system changes to update, improve, or resolve weaknesses are usually released via a patch.  Security awareness guidelines include the timely installation of security patches as well as implementing vulnerability assessment and vulnerability management.

**Removable Media:** are storage devices that could be added or removed from a running computer, such as CDs, DVDs, removable SD cards, and USB drives (including flash drives, thumb drives, external hard drives). Security awareness guidelines include drive encryption and following the policy and guidelines presented at the organizational level regarding the use of personal removable media on organizational systems.

**Safe Web Browsing:** Security awareness guidelines regarding securely navigating websites include looking for the padlock icon on the URL bar before entering sensitive information like credentials, credit card information, or personally identifiable information.  Another visual indicator is "https" reflecting in the web address. The padlock and "https" indicate that the entered information will be secure. Lastly, guidance could be shared to set privacy options on the browser or use the incognito option to limit the information shared. Yet another guideline is to consider using a virtual private network (VPN).

**Social Engineering** involves interacting with humans in hopes that they will disclose sensitive information. Security awareness guidelines include not opening suspicious emails from unrecognized senders, not clicking on suspicious links in emails or on websites, not opening attachments in emails, not disclosing information, and not responding to suspicious emails or contacts provided therein.

I also prepared an interview for cyber security teacher Igor Burger, who as a teacher I regard as an expert on the topic. The goal of the interview is to get his insights on cyber security awareness and confirm the information I found. This can be found in the following document: Interview on cyber security awareness

<https://www.cyberpilot.io/nl/cyberpilot-blog/11-tips-voor-een-succesvolle-security-awareness-training> This was an interesting source; it discusses some of the tips on making a cyber-security awareness training. I could use this later when designing the game.

After discussing this all with the stakeholder, we came to the conclusion that the game should be about social engineering and phishing.

# Results

With this information, I gathered the following:

* The game should cover the topics of social engineering and phishing. These topics are the ones that users have the most control over in terms of own security. This has also been discussed with the client and agreed upon.
* The rest of the information (such as the ways hackers use to apply social engineering) can be used in the game itself.