THE EU CYBERSECURITY AGENCY

WHAT IS SOCIAL ENGINEERING AND WHY IS IT A THREAT?

EUROPEAN CYBER SECURITY MONTH

Target Audience: eTwinning teachers **Subject:** Social Engineering

According to the Oxford Dictionary, social engineering is "the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes."[1]

Social engineering techniques are frequently used by online criminals to trick victims into trusting them, and then obtain information they need to fully perpetrate their crimes.

Recent research[2] found that 2/3 of victims of identity theft and impersonation were identified as having been compromised through a data breach or through social media.

The video (data to go) shows just how much information can be gleaned by simply "liking" a Facebook page.

1 https://en.oxforddictionaries.com/definition/social_engineering

2 https://www.cifas.org.uk/secure/contentPORT/uploads/documents/Internal-Wolves%20of%20the%20Internet%20Final.pdf

How (silly and sophisticated) social engineering works

Take a look at this video (https://www.youtube.com/watch?v=UzvPP6_LRHc). This is an example of silly social engineering. But some attackers are really smarter than that, sneakily playing with emotions and making the whole situation look completely normal...watch this sophisticated social engineering video (https://www.youtube.com/watch?v=lc7scxvKQOo), in which this talented woman hacker accesses a poor man's account by tricking his customer service!

When people are most likely to be victim of social engineering

It could look like a message (or an email) from an (alleged) best friend suggesting that you check out a fun app.

Or your favourite game telling to download a great new game.

Or an advert on Facebook offering discounted tickets to see a great artist which appears to be endorsed by a friend.

THREE RULES[3] ON HOW TO NOT BE TRICKED BY SOCIAL ENGINEERS

1. Never send confidential information to anyone, be careful when you share personal data

No credible online service will ever ask for username and password in a different situation than the app or the website's login page. Likewise, a bank will never ask you to send credit card details by email. If in doubt you should go to the genuine website of your bank – do this by typing in the URL (web address) rather than by clicking on a link provided in an email as these will often take you to a page which looks genuine but which is not.

NO CREDIBLE ONLINE SERVICE WILL ASK FOR YOUR CREDENTIALS IN A DIFFERENT SITUATION THAN THE APP OR THE WEBSITE'S LOGIN PAGE.

Usually, websites or apps will ask for some personal data like name and surname, home and email address, maybe an identification number, in order to sign you up to their services, but before providing this information, think about this question: do you trust the site to handle your data properly? If it looks a bit dodgy, maybe you should look for a more reliable service that someone like parents or teachers can recommend?

3 Information was collated from https://www.social-engineer.org/; https://www.esecurityplanet.com/views/article.php/3908881/9-Best-Defenses-Against-Social-Engineering-Attacks.htm; https://www.webroot.com/ie/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering; https://www.ed.ac.uk/infosec/how-to-protect/social-media-protection/social-engineering.

2. Be critical

When any kind of information online is seen or received, it is important to be critical and vigilant. Two things are really important to check out if you want to detect possible scams: context and the person/service interacting with you.

Examples for teachers

Tell your students to be cautious about things online that appear out of the blue and seem too good to be true.

Some examples

First, is the context feasible? If an online advert or an email encourages you to buy a newly released videogame for only 9,99 euros despite the fact that it actually costs 70 euros pretty much everywhere else, should you believe it? Why would they sell it for such a discounted price? If it looks too good to be true then it probably is.

Second, is the person you are interacting with credible? If a "university admission expert" promises to get you into your dream university, what are his or her "experts' credentials"? Why is he or she putting pressure on you to make that online payment, if admissions deadlines are literally in a year? And, how does he or she know you really want to go get into these three programs that only you and your parents know about?

Check this link for a story that actually happened to see what went wrong

IF IT LOOKS TOO GOOD TO BE TRUE, THEN IT PROBABLY IS!

3. Be extremely cautious about what you share online

People should be aware of what they post online and what is shared in general.

For example, there are programs that can aggregate what one posts/uploads online. They are called **social network aggregator software** and sometimes they are used to gather as much information as possible about a person, before sending a carefully planned social engineered attack.

Take a look at this video to understand how much all of us share online (https://www.youtube.com/watch?v=F7pYHN9iC9I).

When creating a social media account, it is important to use privacy settings and take control of what is being shared. Open (or public) profiles are not a good idea. Behind a cute puppy profile picture, there might be someone bad who is interested in something more than an online friendship. You do not know what these bad people will do with the information they obtain online, but they certainly do.

For an extra layer of privacy

learn more about social engineering

The best way to avoid falling victim of social engineers is to know more about their practices. Social-engineering.org (https://www.social-engineer.org/) has an information section for people to learn more about the psychological, physical and historical aspects of social engineering. The two subsections on "common attacks" and "real world examples" are good to gain a better understanding how social engineers operate. The blog is also informative.

Find more resources on the Better Internet for Kids portal!

More cyber hygiene resources in various European languages can be found at the Better Internet for Kids portal. Check out the #SaferInternet4EU campaign page.