Online safety versus Cyber security

By Kim Vernon, December 2021

With so many technical terms in Digital Technologies, we often find ourselves using certain terms in an interchangeable fashion. One example of this is online safety and cyber security. Words used as often as 'security' and 'safety' should have well-understood definitions. Both words are associated with being free from harm.

Let's dig a little deeper, what is the difference between online or cyber safety and cyber security?

Online safety and cyber security are related, and both involve online safety. But they have important differences:

- cyber safety involves protecting people when they are online
- cyber security involves protecting data or information and keeping it safe, secure from hackers and attackers.

*To understand more about who hackers and attackers are and the roles they play in the security of systems, see the DTiF resource Teaching Tips – Hacker versus Attacker

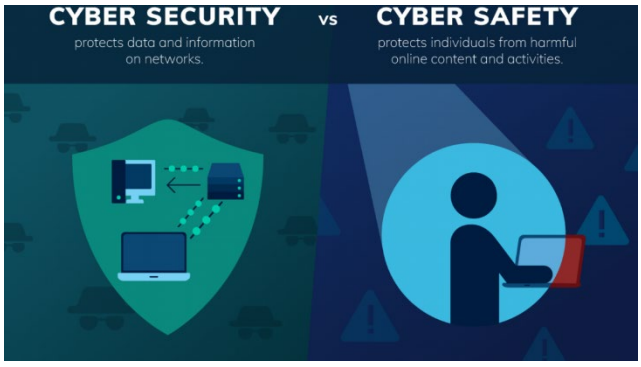

Image source:
https://www.paulfletcher.com.au/blog/cyber-safety-and-cyber-security-whats-the-difference

- Being cyber or online safe means meeting appropriate standards of behaviour in the content we put on the internet, knowing how to avoid harmful interactions online, and being equipped to seek help if things don't seem right.
- Cyber security refers to the physical operation of the networks and computers over which the internet is delivered.

If an attacker obtains remote control of your computer and alters lines of code in its operating system; if a company's network fails because hundreds of thousands or even millions of messages are directed at it by computers around the world; if a virus freezes all of your data and criminals, then contact you offering to unfreeze the data if you pay a ransom – those are all cyber security issues.

The role humans play in cyber security

Cognitive vulnerabilities play a major role in how successful cyber security may be in a home or work network. Cognitive vulnerabilities identify the critical role human behaviour plays in cyber security and provides insights into how human decision-making can help strengthen or weaken a system's defence. The bias that we as humans bring when designing, building, programming, and using digital systems can influence the effectiveness of cyber security. Cognitive bias is an error in the thinking process that affects decision-making. Studies on the subject show that attackers target cognitive bias in combination with technical flaws to exploit a system successfully.

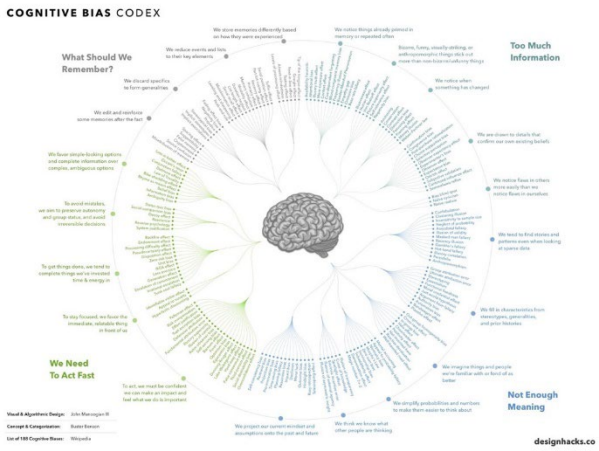

Image source: https://www.visualcapitalist.com/wp-content/uploads/2021/08/all-188-cognitive-biases.html

Examples of cognitive bias in action

The Ostrich effect

This type of bias is often associated with avoiding negative information, including feedback. If we display this bias during the design phase of a system, where user feedback has indicated, a change is needed to better secure the system, we run the risk of sending a system out for production which has serious gaps in security. You often see software companies sending ‘patches’ out for users to download. Operating system updates are frequently needed, these are usually to ‘patch’ a gap in the security of the system.

Overconfidence effect

The overconfidence effect is observed when people's subjective confidence in their ability is more significant than their objective (actual) performance. There are reasons to believe that the sinking of the Titanic was very much due to this bias. The overconfidence effect can trick people into making bad decisions and create a false sense of security. Overconfidence in the security of a system because of firewalls or antivirus could ultimately result in severe security breaches.

Confirmation bias

Confirmation bias is the tendency to search for, interpret, favour, and recall information in a way that confirms or strengthens one's prior personal beliefs or hypotheses. Confirmation bias can trick the mind into only looking for specific issues related to an IT infrastructure, based on one's previous experience and understanding, instead of considering security as a whole. The unwritten rule in cyber security is "never assume”.