TOP 5 SPOOKIEST CYBERSECURITY THREATS

Trick or Threat?

1. SOCIAL ENGINEERING

Techniques used by hackers to trick people into disclosing or volunteering confidential information, or to take certain actions.

2. RANSOMWARE ATTACKS ON THE CLOUD

Encrypt your cloud storage, and then demand ransom payment.

3. PHISHING

Luring someone (usually via email) into sharing sensitive information or downloading malware.

4. HUMANS

Fallible creatures who make mistakes, can be manipulated, and are not always aware of the latest security threats.

5. MINING CRYPTOCURRENCIES

Mining cryptocurrencies requires plenty of computing capacity, and hackers are hijacking computers to do so.

DON'T LET THEM SCARE YOU! HERE IS WHAT YOU CAN DO TO DEFEND YOURSELF

1. **Social engineering:** Use common sense, and never, ever give away your username and passwords! A good anti-virus software will help keep you safe.

2. **Ransomware attacks on the cloud:** Never forget to regularly back up your data locally and in the cloud, possibly in multiple locations. This way you will not lose access, even if you fall victim to ransomware.

3. **Phishing:** Educate yourself on how to spot phishing emails: be suspicious if the message was sent by a generic recipient, interpret bad grammar as a red flag, and hover with your mouse on all the links to verify their legitimacy.

4. **Humans:** Train your humans! Keep up to date with the most common security threats and raise awareness of risks by talking to your family, friends and colleagues.

5. **Mining cryptocurrencies:** Use a good anti-virus software to protect your OS and an ad-blocker to protect against miners in your web browser.