pretexting  cybercrime  breach
malware  spoofing  socialengineering
scam  phishing
data  twofactorauthentication
Term Definitions

1. **Phishing** - type of scam where hackers use deceptive emails and messages to gain information (ex. Passwords, bank account numbers)

2. **Malware** - Malicious software that damages or gains unauthorized access to computer systems or data (ex. Phishing emails can contain malware)

3. **Scam** - broader category of fraudulent activities that try to deceive individuals and their sensitive information (ex. phishing, phone scam)

4. **Data** - any electronically stored information, often targeted by hackers

5. **Cybercrime** - Criminal activities carried out using computers or the internet, often involving hacking, fraud, and identity theft

6. **Spoofing** - Falsifying communication information to appear as though it is coming from a legitimate source. (ex. used in phishing attacks for deception)

7. **Pretexting** - social engineering tactic in which a fake scenario is created to gain confidential information (ex. posing as a bank representative to obtain account details)

8. **Two-factor authentication** - requires a password and a secondary verification, like a code sent to a mobile device, reducing the risk of unauthorized access, especially from phishing. (ex. Duo push)

9. **Breach** - security incident where unauthorized access or compromise of systems or data occurs (ex. sometimes started by phishing attacks)

10. **Social Engineering** - psychological manipulation techniques used by hackers or in phishing emails to deceive individuals into giving confidential information (ex. Phishing, pretexting)