Task 2: Cards and Payments

Payments

- Modern payment cards use chips because they offer much better security than magnetic stripes. Magnetic stripes store static data, which can be easily copied by criminals using a method called "skimming." once the data is copied, the card can be cloned and used illegally. EMV chips, on the other hand, create a unique transaction code every time the card is used. This makes it nearly impossible for fraudsters to replicate the card and use it elsewhere, which significantly reduces the risk of fraud.
- EMV certificates are a key part of the security framework used in chip-based cards. They help verify the authenticity of the card when it's used in a transaction. This means that each transaction involves a cryptographic check between the card and the terminal, ensuring the card hasn't been tampered with or cloned. This level of verification is what helps protect against many types of fraud, making it a crucial part of modern payment security.
- What attacks exist against payment cards?
  - Card-not-present fraud: This happens when someone uses your card details to make purchases online or over the phone, where the physical card isn't needed.
  - Contactless payment attacks: Although rare, attackers could potentially intercept signals from contactless cards, but modern encryption makes this difficult. Other risks include unauthorized small transactions if a card is lost and someone uses it before it's blocked.

Questions: MFA

- In banking, MFA is used to secure access to online accounts and transactions. For example, after entering a password, you might need to confirm a code sent to your phone or use a fingerprint to complete a login or transfer funds. This adds an extra layer of security, making it much harder for someone to hack your account because they would need more than just your password.
- MFA boosts payment security by requiring more than one way to verify your identity. Even if a hacker manages to steal your password, they still can't get into your account without access to the second factor, like your phone or fingerprint. This means there are more barriers for attackers to break through, making your accounts and payments safer.
- In daily life, MFA methods can include: time-based one-time passwords: these are codes generated by an app, like Google Authenticator, which change every 30 seconds.
  SMS codes**:** temporary code sent via text message to your phone.
  Biometrics: using your fingerprint or face ID to unlock devices or log in to accounts.
- What attacks exist against different forms of 2FA?

  -TOTP attacks: Although safer, these codes can still be intercepted if your phone or authenticator app is compromised. **SMS-based attacks:** Hackers can exploit weaknesses through methods like SIM swapping, where they take control of your phone number and intercept your SMS codes. They might also use malware to access the messages directly.