Questions: Payments

- Why do modern payment cards use a chip and not a magnetic stripe?

The chip is a microcircuit that stores the cardholder's data in an encrypted format. This makes it much more difficult for fraudsters to steal the data and use it to make unauthorized purchases. Also, Chip cards are more difficult to counterfeit, skim, difficult to alter and offer better protection against fraud.

For the magnetic stipe card, it is very easy to clone them and steal information from them.

- What are EMV Certificates and why are they relevant for payment protection?

EMV certificates are used to verify the authenticity of the card and the terminal during an EMV transaction. They are important for payment protection because they help to prevent fraud in many ways, like;

- They help to prevent counterfeit cards from being used.
- They help to prevent lost or stolen cards from being used.
- They help to prevent unauthorized transactions from being made.
- They help to protect merchants from fraudulent chargebacks.

EMV certificates are issued by trusted third-party organizations, such as VeriSign and GlobalSign. These organizations verify the identity of the card issuer and the terminal operator before issuing a certificate.

When an EMV transaction is made, the card and the terminal exchange certificates. The terminal then verifies the certificate of the card issuer. If the certificate is valid, the terminal can be confident that the card is authentic.

EMV certificates are an important part of the EMV security system. They help to protect payments from fraud and make EMV transactions more secure.

- What attacks exist against payment cards?

  - **Card stealing:** This is a common attack where the thief steals the victim's card and then uses it to make fraudulent purchases. This attack can be prevented by keeping your card safe and not giving it to anyone you don't trust.
  - **Card cloning:** This attack involves copying the magnetic stripe on a victim's card to a blank card. The thief can then use the cloned card to make fraudulent purchases. This attack can be prevented by using a card with a chip and PIN.

- **EMV chip card attacks:** One common attack is to counterfeit the chip on an EMV card. Another attack is to use a malware-infected terminal to steal data from the chip on an EMV card.

- Card-not-present?

  Card-Not-Present transactions are vulnerable to a number of attacks, including social engineering attacks, phishing attacks, and malware attacks.

  Social engineering attacks involve tricking the cardholder into revealing their card information, such as by posing as a legitimate company or organization. Phishing attacks involve sending fraudulent emails or text messages that appear to be from a legitimate company or organization, in order to trick the cardholder into clicking on a link that will take them to a fake website where they will enter their card information. Malware attacks involve infecting the cardholder's computer with malware that can steal their card information.

- Contactless payment?

  Relay attack: In this type of attack, the attacker uses two devices, one to skim the data from the contactless card and the other to transmit that data to a nearby terminal. This could allow the attacker to make a payment without the cardholder's knowledge or consent.

  Man-in-the-middle attack: In this type of attack, the attacker intercepts the communication between the contactless card and the terminal. This could allow the attacker to steal the cardholder's data or even make a fraudulent payment.

  Clonning: This could be done by stealing the data from a contactless card and then using that data to create a new card.

Questions: MFA

- How is multi-factor authentication (MFA) used in banking?

Multifactor authentication (MFA) is a security measure that requires users to provide two or more factors to verify their identity. This can include a password, a one-time code from a mobile app, or a fingerprint scan. MFA is used in banking to protect customer accounts from unauthorized access. It can be used as :

- To login into a bank account online, users may be required to enter their password and a one-time code from a mobile app.
- To make a large transaction, users may be required to enter a one-time code from a mobile app or a fingerprint scan.
- To transfer money to a new account, users may be required to enter a one-time code from a mobile app or a fingerprint scan.

- How does multi-factor authentication increase payment security?

MFA is effective at increasing payment security because it makes it much more difficult for fraudsters to gain access to a user's account and make fraudulent payments. Even if a fraudster is able to obtain the user's password, they would still need to have access to the user's mobile phone or security key in order to complete the payment.

It also reduces the risk of account takeover as it can help to prevent fraudsters from taking over a user's account by requiring them to provide additional evidence of their identity when logging in.

It protects against phishing attacks. It can help to protect users from phishing attacks by requiring them to provide additional evidence of their identity when making a payment.

MFA also mitigates the impact of data breaches. If a user's password is compromised in a data breach, MFA can help to prevent fraudsters from using that password to access the user's account and make fraudulent payments.

- What MFA methods are you using in you daily life?

I am using three MFA methods in my daily routine:

One-time password (OTP): I am using OTP method for Moodle Login and for bank transactions.
Biometric authentication: I am using fingerprint and face scan, for some applications, like to login in LinkedIn.
Authenticator Application: I am using Microsoft Authenticator application and Google Authenticator application also for more security.

- What attacks exists against different forms of 2FA?
    - **Phishing attacks**: Phishing attacks are attempts to trick users into revealing their personal information, including their 2FA codes. These attacks can be carried out through email, text message, or even social media.
    - **Man-in-the-middle attacks:** Man-in-the-middle attacks involve the attacker intercepting communication between the user and the service they are trying to access. This can be done by creating a fake login page or by compromising the user's network connection. Once the attacker has intercepted the communication, they can steal the user's 2FA code or even log in to the service themselves.
    - **SIM swapping attacks:** SIM swapping attacks involve tricking the user's mobile carrier into transferring their phone number to a SIM card controlled by the attacker. This can be done by social engineering the carrier employee or by exploiting a vulnerability in the carrier's system. Once the attacker has control of the user's phone number, they can receive any 2FA codes sent to that number.
    - **Malware attacks:** Malware attacks can be used to steal 2FA codes from the user's device. This can be done by installing a keylogger on the device or by exploiting a vulnerability in the device's operating system.
    - **Weak 2FA implementations:** Some 2FA implementations are simply more secure than others. For example, SMS-based 2FA is relatively insecure because SMS messages can be intercepted. More secure forms of 2FA include authenticator apps and hardware security keys.

- Time-based-one-time-password (TOTP)?
    - **Phishing**
    - **Man-in-the-middle attacks**
    - **Replay attacks:** Replay attacks involve reusing a previously valid TOTP code. This can be done if an attacker is able to capture a TOTP code that a user sends to a service, and then send that code to the service later to gain access.
    - **Seed compromise:** TOTP codes are generated using a shared secret, known as a seed, that is shared between the user's device and the service that they are authenticating to. If an attacker is able to compromise the seed, they will be able to generate valid TOTP codes at will.

- Text Message?
    - **SIM swapping:** This is a type of attack where the attacker tricks the victim's mobile carrier into transferring the victim's phone number to a SIM card under the attacker's control. Once the attacker has control of the victim's phone number, they can intercept all SMS messages, including 2FA codes.
    - **Phishing**
    - **Man-in-the-middle attacks**
    - **Malware**