8/ Secure File Transfer

Things to consider

Transferring files over the internet is another form of online communication, and most of the same vulnerabilities and protection tactics apply. There are a number of additional issues with email attachments, online file sharing, and cloud services, to be aware of.

- Email attachments are a common way to spread **malware**, including targeted malware. Malicious actors sometimes even send encrypted attachments; be especially suspicious of emails which include the password to decrypt the attachment.
- Many common file-sharing or cloud platforms offer **only SSL encryption** to protect the data exchanged over these platforms. SSL encryption has several vulnerabilities which have been exploited to access user data. Furthermore, it often allows owners of the platform to access the content shared by users and their data for their own interest, or as requested by authorities.
- The backup functionalities on phones, tablets, or computers generally store backed-up content **without encryption on their servers.**

Protection tactics

- Verify unexpected or suspicious files sent to you: check over a third, secure channel what was sent, and why.
- Use tools for secure communication that implement **end-to-end encryption.** This can reduce the likelihood of a malicious actor successfully fooling you into thinking an attachment was sent by a legitimate contact.
- Verify the **security numbers or fingerprints** associated with different devices via a third channel or during in-person meetings. This helps to prevent social engineering or ‘man in the middle’ attacks.
- Use **file-sharing and cloud services** which offer end-to-end encryption and share passwords over a third secure channel with your contacts if necessary.
- When using unencrypted cloud services such as Dropbox, make sure to **encrypt data before storing it** online.