Essential Guide to Digital Theft

Phishing Scams

How to spot them:

- Seemingly legitimate email or pop-up requesting personal info, password, or to install software
- May come from known legitimate email contacts, or senders disguised to look like family and friends
- Usually unsolicited, comes without warning

How to avoid them:

- Do not click links or respond to email
- Delete email and/or block sender
- If the email is coming from a known contact in your address book, call them at a known phone number to warn them they are being impersonated by a scammer

Tech Support Scams

How to spot them:

- Unsolicited emails, calls, or pop-up windows offering tech support
- Request for access to your device (passwords, personal information)
- Insistence that your computer has been "hacked" and only they can help you

How to avoid them:

- Ignore emails, calls, or pop-ups that say your computer is infected
- Do not share personal or financial information with strangers.
- Do not share passwords

Ransom for File Scams

How to spot it:

- Computer suddenly locked and you can't access files
- Receive a message requesting money or they will delete your files
- Unable to use computer or close ransom message even after restarting

How to avoid it:

- Keep a secure backup of your device to avoid file loss
- Remember that there is no guarantee that paying ransom will return files
- File a police report

Online Dating Scams

How to spot it:

- Online suitor quickly professes their love for you without meeting in person
- Will not meet in person for various reasons
- Requests money or personal information to solve a pressing problem

How to avoid it:

- Do not share personal information or payments with online dates
- Frequent spelling errors or early declaration of love is a red flag
- Report fraudulent or suspected accounts

Family Member in Trouble Scams

How to spot it:

- Email or message that appears to come from a family member in trouble
- Request for immediate payment, usually via wire transfer
- Message will have family member's name attached and appear legitimate

How to avoid it:

- Call family member at a known phone number to verify they are okay
- Do not send money or share financial information via email, phone, or messaging
- Delete any emails or messages from attacker