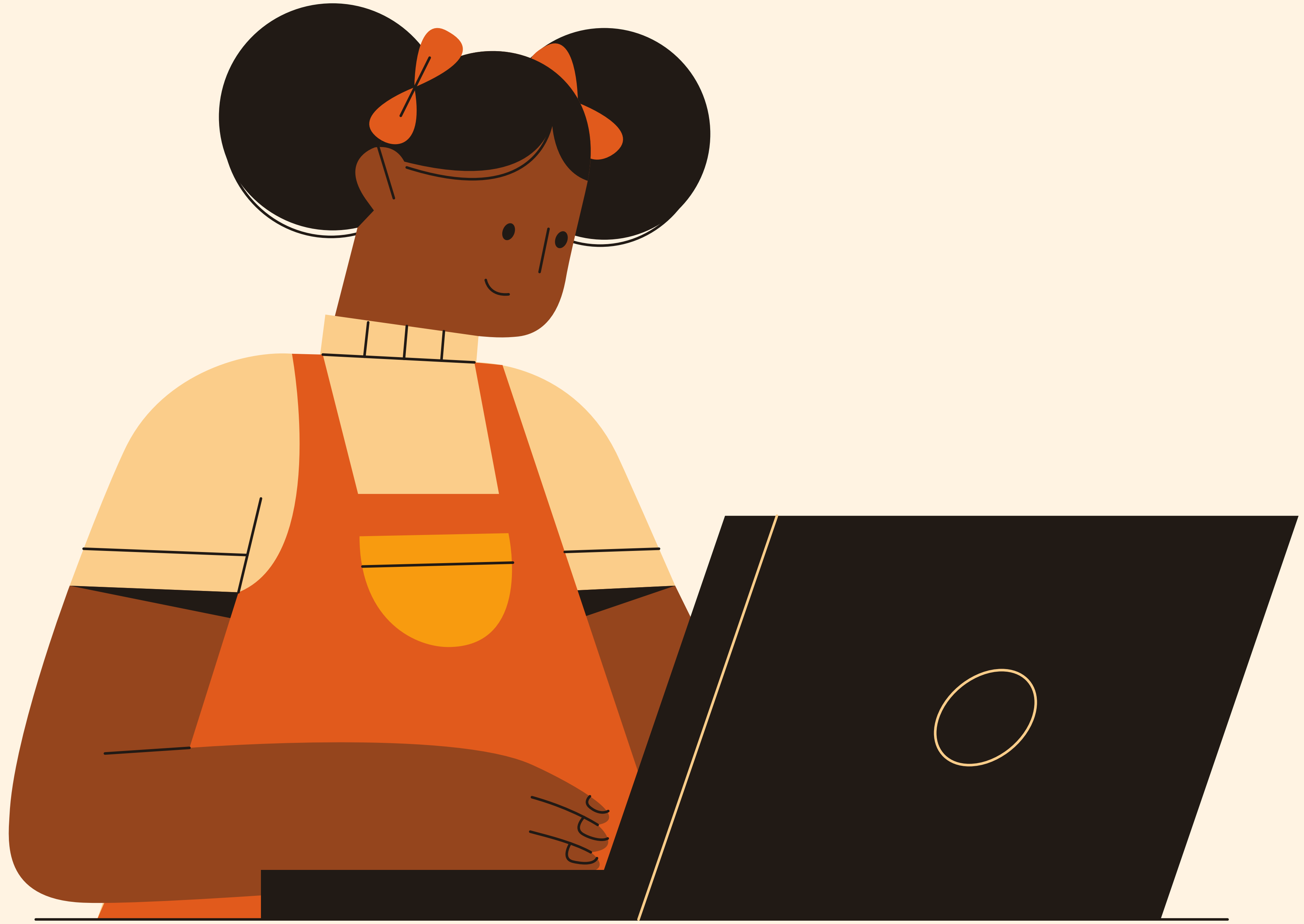
SECURING PERSONAL DEVICES



Presenters:
Ali Hassan
Muzfar Baloch

What is personal cyber security?

In an increasingly tech-driven world we use devices and accounts every day that are vulnerable to cyber threats.

- Your devices may include computers, mobile phones, tablets and other internet connected devices.
- You also may use online accounts for email, banking, shopping, social media, gaming and more.

Personal cyber security is the continuing steps you can take to protect your accounts and devices from cyber threats.

GUIDE HELP PROTECT ME FROM CYBER THREATS?

Turn on automatic updates

Software updates help protect your devices by fixing software ‘bugs’ (coding errors or vulnerabilities). Cybercriminals and malware can use these ‘bugs’ to access your device and steal your personal data, accounts, financial information and identity.

- New software ‘bugs’ are constantly being found and exploited by cybercriminals. Updating the software on your devices helps protect you from cyber-attacks.

ACTIVATE MULTI-FACTOR AUTHENTICATION (MFA)

Two-factor authentication (2FA) is the most common type of MFA, requiring two different authentication types.

You can use multi-factor authentication (MFA) to improve the security of your most important accounts. MFA requires you to produce a combination of two or more authentication types before granting access to an account.

MFA makes it harder for cybercriminals to gain initial access to your account. It adds more authentication layers, requiring extra time, effort and resources to break.

Use passphrases to secure your important accounts

What is a passphrase?

A passphrase uses four or more random words as your password. For example: 'crystal onion clay pretzel'.

- Passphrases are more secure than simple passwords
- Passphrases are hard for cybercriminals to crack, but easy for you to remember

Device Security

- Lock your device with a passphrase, password, PIN or passcode. Make it difficult to guess – your date of birth and pattern locks are easy for anyone to guess. Use a passphrase for optimal security. You might also consider using facial recognition or a fingerprint to unlock your device.
- Ensure your device is set to automatically lock after a short time of inactivity.
- Don't charge your device at a public charging station and avoid chargers from third parties.

Treat your phone like your wallet. Keep it safe and with you at all times.

Data Security

- Enable the remote locking and wiping functions, if your device supports them.
- Ensure you thoroughly remove personal data from your device before selling or disposing of it.

HOW DO I RECOGNISE SCAM MESSAGES?

It can be difficult to recognise scam messages. Cybercriminals often use certain methods to trick you. Their messages might include:

- Authority: is the message claiming to be from someone official, such as your bank?
- Urgency: are you told there is a problem, or that you have a limited time to respond or pay?
- Emotion: does the message make you panic, hopeful or curious?
- Scarcity: is the message offering something in short supply, or promising a good deal?
- Current events: is the message about a current news story or big event?

Tip #1

Only use devices in common areas around the home.

Tip #2

Never share intimate photos with anyone and report to a trusted adult if they are shared with you.

Tip #3

Only communicate and accept friend requests from people you know personally.

Tip #4

Limit your screen time and remember to invest time in human relationships too.

Tip #5

Be mindful of the personal information you share online.

Tip #6

Keep passwords and log in information private.

Tip #7

Think before you type:

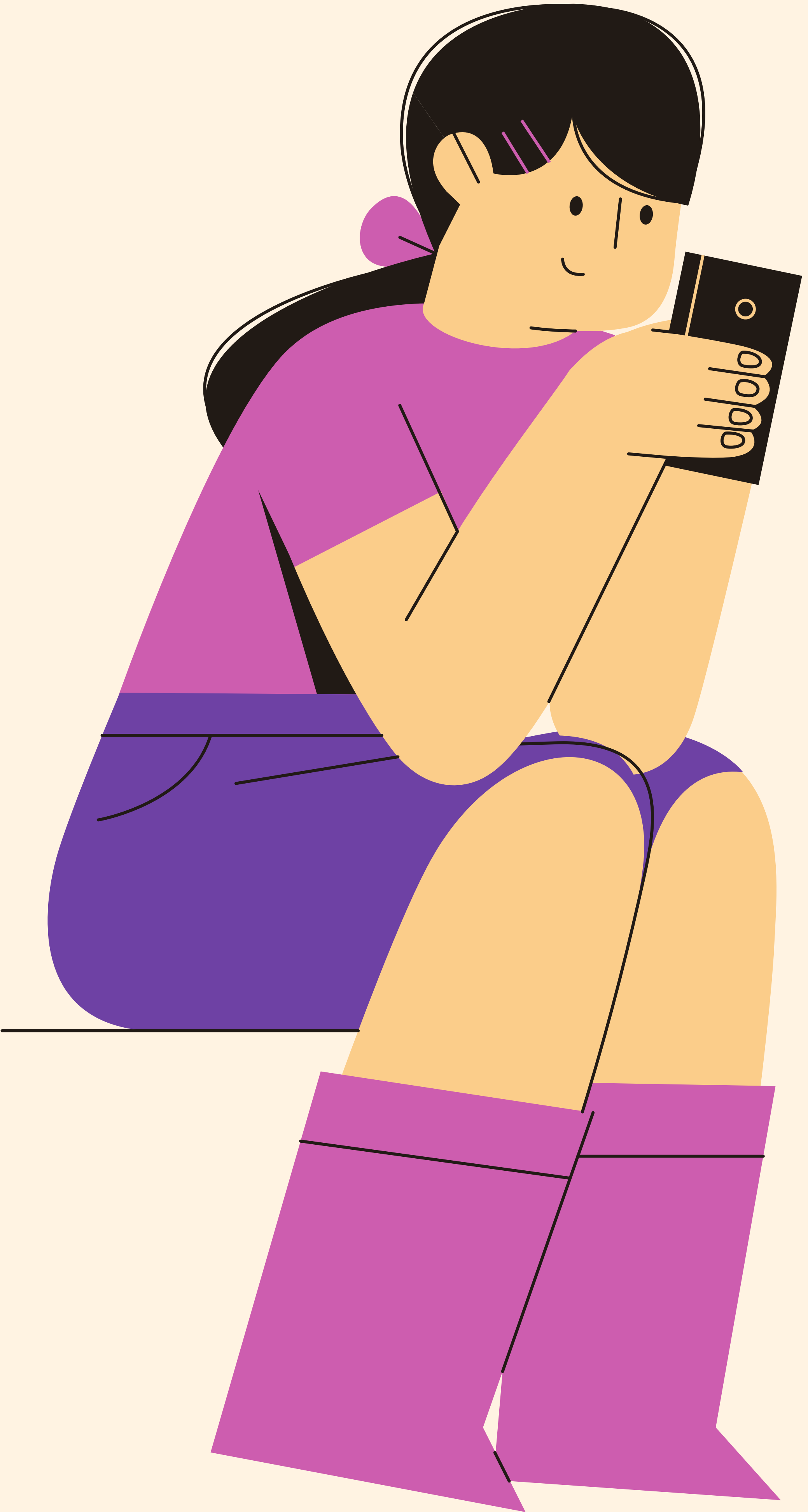
T: is it TRUE?

H: is it HELPFUL?

I: is it INSPIRING?

N: is it NECESSARY?

K: is it KIND?



Tip #8

Be mindful of who you accept files from.

Tip #9

Check the source of information for reliability.

Tip #10

Do not meet up with people you do not know personally or without a trusted adult's permission.

Tip #11

Do not meet up with people you do not know personally or without a trusted adult's permission.

WINDOWS HARDENING

Privacy

- Disable communication with unpaired devices
- Disable activity history
- Disable location access
- Disable ad tracking
- Disable cortana

WINDOWS HARDENING

Security

- **Use standard user**
- **Turn on updates**
- **System Restore**
- **Data Backup**
- **Anti Virus and Firewall**
- **Password Managers**
- **Encryption**

Q & A

What do you want to know about cyber safety?