1

THE LEADER IN SECURITY OPERATIONS

The Internet

- It's Free*
- Connect around the world in seconds
  - Access / search information
  - Talk to friends & family
  - Social media
  - Watch videos (streaming)
  - Listen to music
  - Shop when you want, from where you want!
- Reach countries you could never easily get to - *everywhere is available!*
- The possibilities are endless….!

*Often pay to access the internet (mobile phone / broadband bills)

4

But Not Everything Is Rosey

5

Kevin Poireault
Reporter, Infosecurity Magazine
Follow @Kpoireault Connect on LinkedIn

An infamous ransomware group has claimed to have compromised sensitive data from a children's hospital in Liverpool, UK.

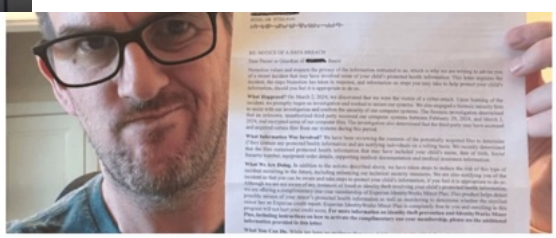
On November 28, INC Ransom posted on its data leak site that it has obtained large-scale data patient records, donor reports and procurement data for 2018-2024 from Alder Hey Children's NHS Foundation Trust.

You may also like

OPINION 2 MAR 2017
Treating Ransomware in the He Sector

NEWS 23 FEB 2024
Operation Cronos: Who Are the Admins?

NEWS 21 NOV 2019



PERSONAL

My child had her data stolen—here's how to protect your kids from identity theft

6

THE LEADER IN SECURITY OPERATIONS

Keeping Safe In The REAL World

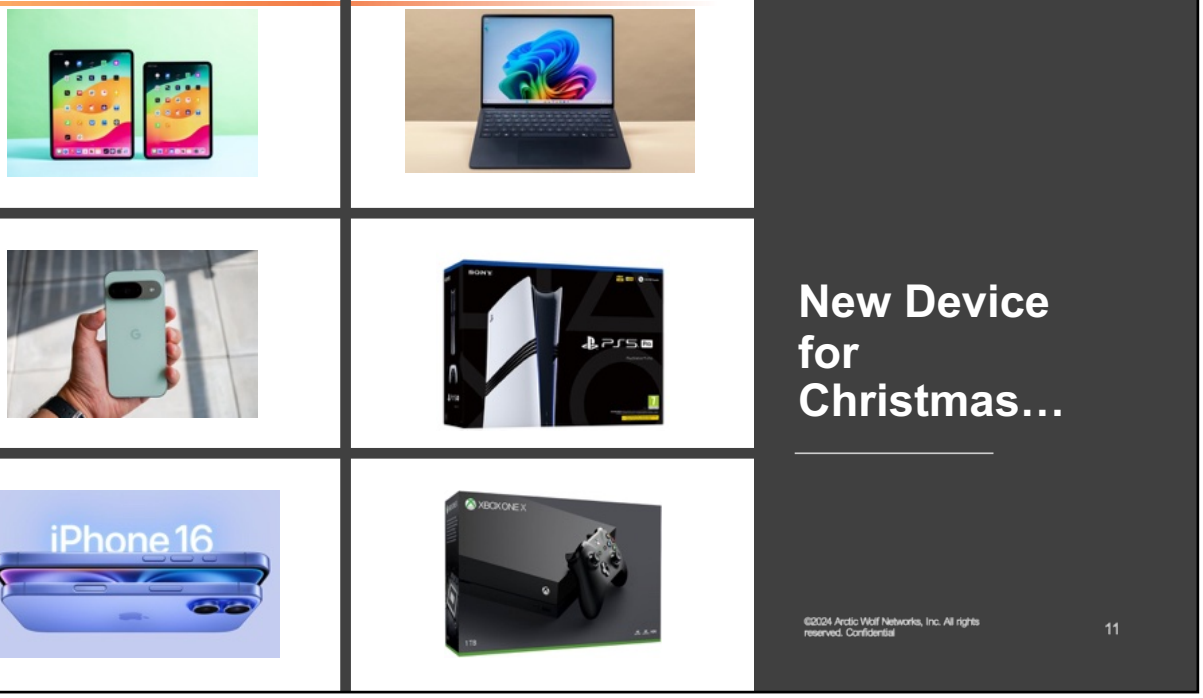
7

THE LEADER IN SECURITY OPERATIONS

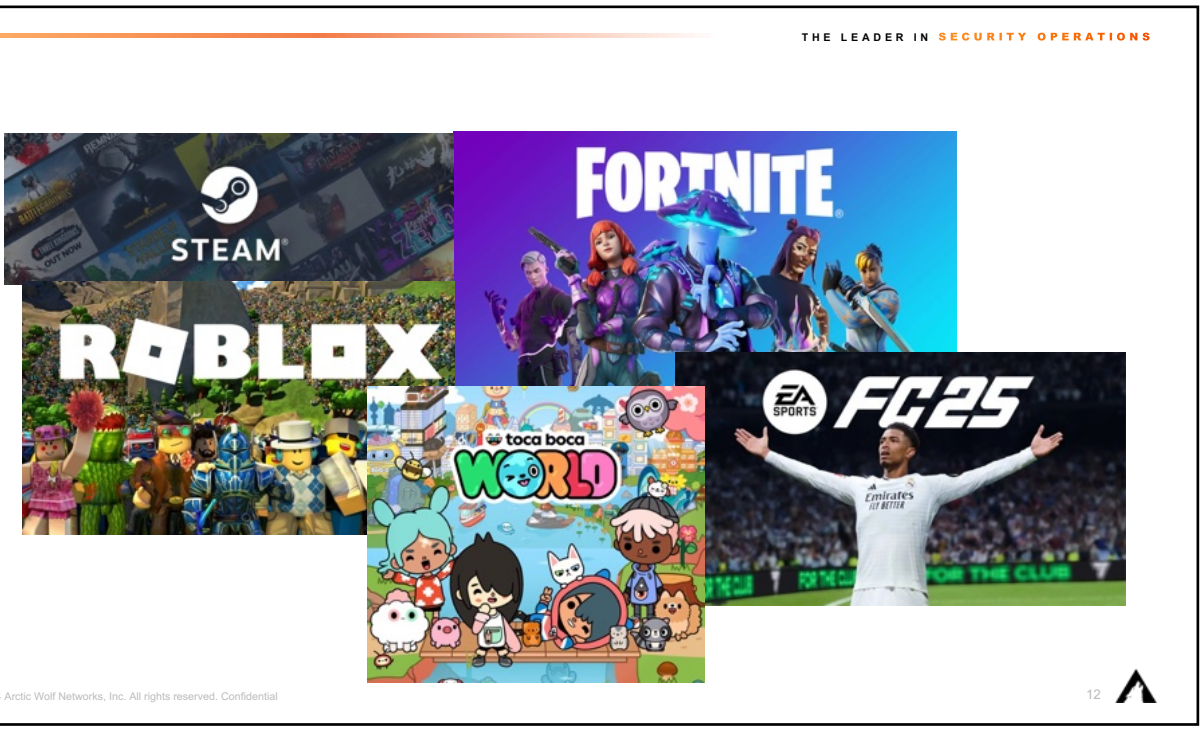
Keeping Safe Online

- The “worldwide web” – everything is interconnected, and you must be aware of the dangers.
- Criminals and bad people act in gangs, and are online to try and take money from you or cause upset.
- A hack of your email can result in your personal secret information being leaked or stolen for everyone to know.
- They can pretend to be you online and post nasty things – your reputation can be damaged
- If they can access your bank, your money can easily be stolen
- **Your digital fingerprint**

8


iPhone 16
New Device for Christmas…
©2024 Arctic Wolf Networks, Inc. All rights reserved. Confidential
11

11


THE LEADER IN SECURITY OPERATIONS
STEAM
FORTNITE
ROBLOX
toca boca
WORLD
EA SPORTS
FC25
©2024 Arctic Wolf Networks, Inc. All rights reserved. Confidential
12

12

Bad Tips / Good Tips

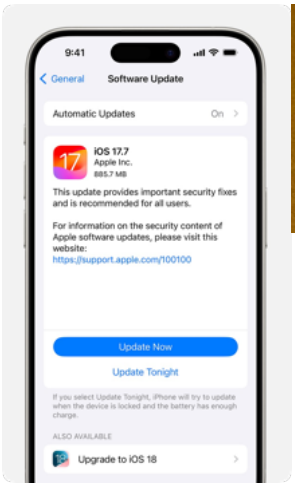
Bad

- Username as your name or about you
- Re-use the same password on each site, or putting ‘1’ at the end
- Allowing strangers to chat with you (that aren’t your friends)
- Giving away your personal details / secrets when asked

Good

- Username purposefully unique and not about you
- Different passwords for each website or gaming platform
- Blocking strangers to chat with you (that aren’t your friends)
- Be cautious!

Update your devices



Social Media

This picture was made with AI… is this correct and to be trusted?

15

15

Social Media & You

- **Promotes a distorted view of the world**
  - Content pushed to you using AI
  - Can make you feel sad – 'not as cool/hip'
  - Ads disguised as user posts making you want to buy things
  - Fake news - displaying opinion as fact
- **"Doomscrolling"**
  - Extremely hard to put away
  - £££

16

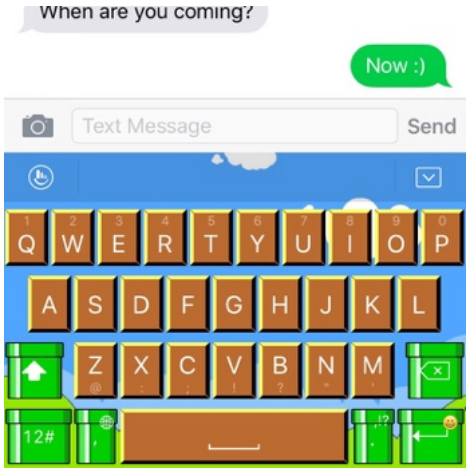
16

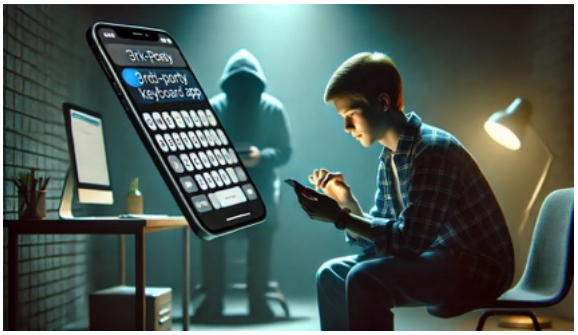
We Are The Product

- Everyone has a digital fingerprint & footprint
- Access to your messages, photos, videos, location, shopping habits, websites you visit
- Generates knowledge about you… that companies want to buy
- **The content you post stay online forever**
- **Cyber criminals can use this to pretend to be you or bribe you to do something!**

17

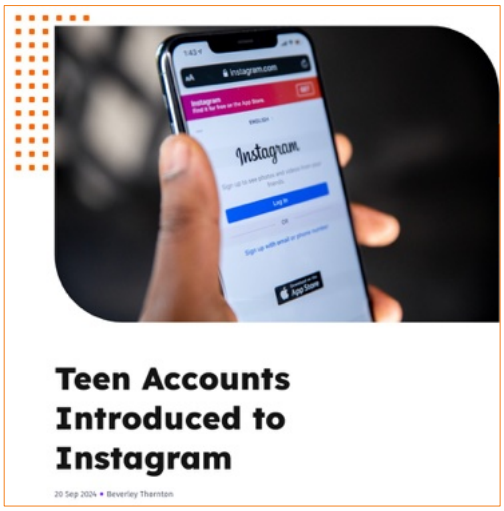
Keyboard Apps – a way to steal your passwords





- Keyboard apps are an easy way for criminals to read everything you type into your keyboard!
- Secrets, conversations, passwords!

18



- Create your own content and feeds
- Set your privacy settings to the highest
- Allow messages from only people you follow
- Have your parents help – we've been through this!

19

Keeping Safe Online

20

4 key ways to defend yourself

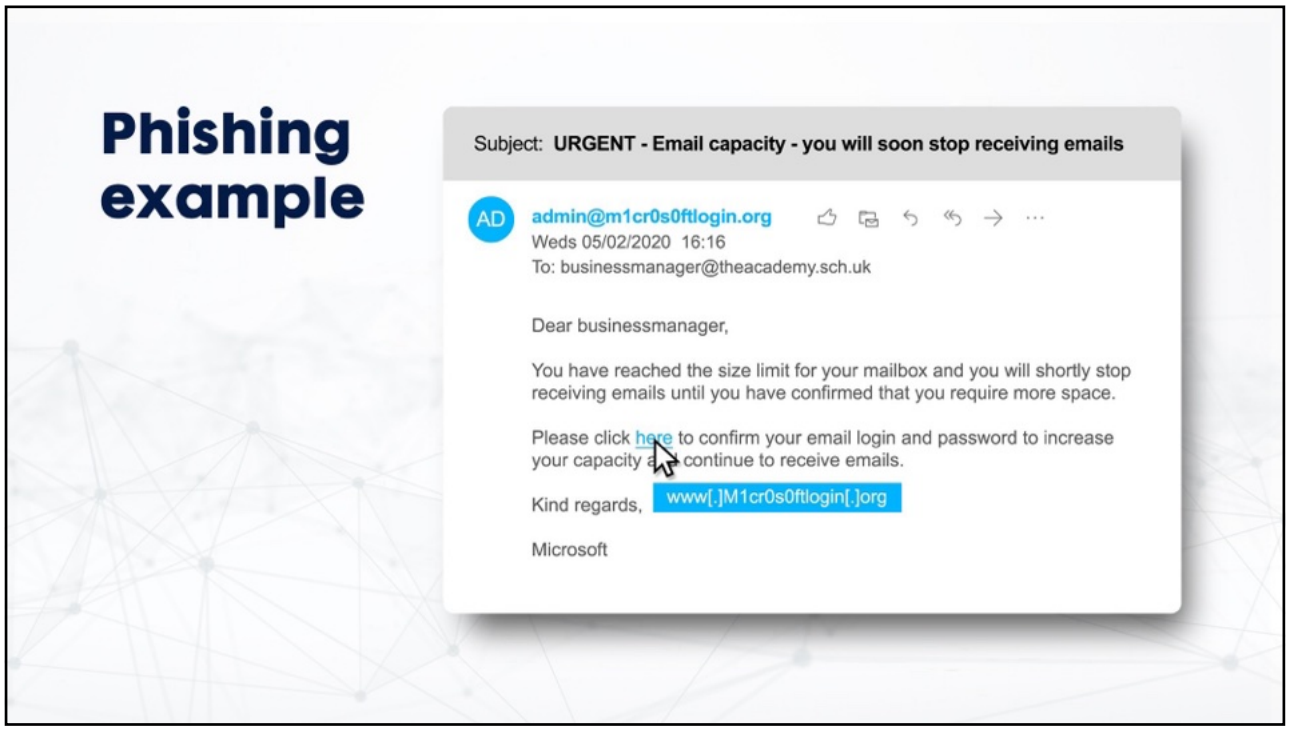
- Defend against phishing attempts.
- Use strong passwords.
- Secure your devices.
- If in doubt call it out.

21

22


National Cyber Security Centre
Phishing
Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
www.ncsc.gov.uk/glossary

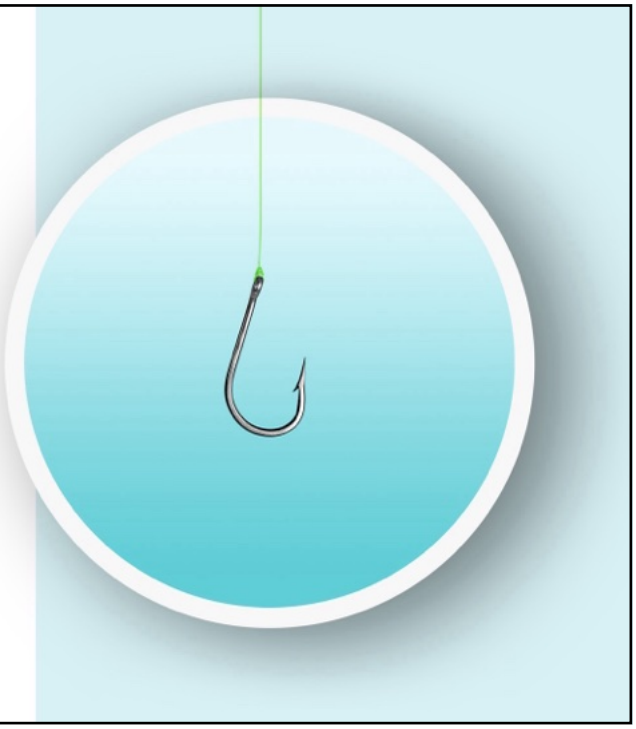
23


Phishing example
Subject: URGENT - Email capacity - you will soon stop receiving emails
AD
admin@m1cr0s0ftlogin.org
Weds 05/02/2020 16:16
To: businessmanager@theacademy.sch.uk
Dear businessmanager,
You have reached the size limit for your mailbox and you will shortly stop receiving emails until you have confirmed that you require more space.
Please click here to confirm your email login and password to increase your capacity and continue to receive emails.
Kind regards,
www[.]M1cr0s0ftlogin[.]org
Microsoft

24

1. How do I defend myself against phishing attempts?

1. Reduce the information available to attackers.
2. Know the influence techniques.
3. Know what 'normal' looks like.
4. Don't be embarrassed to ask for help.
5. Report if you click!



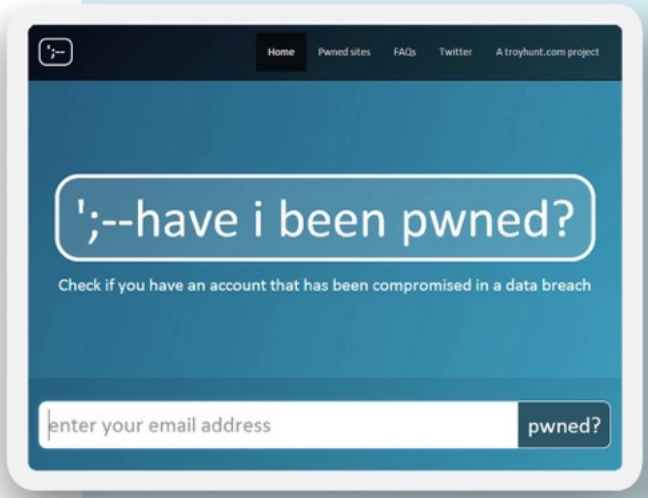
25

2. Use strong passwords

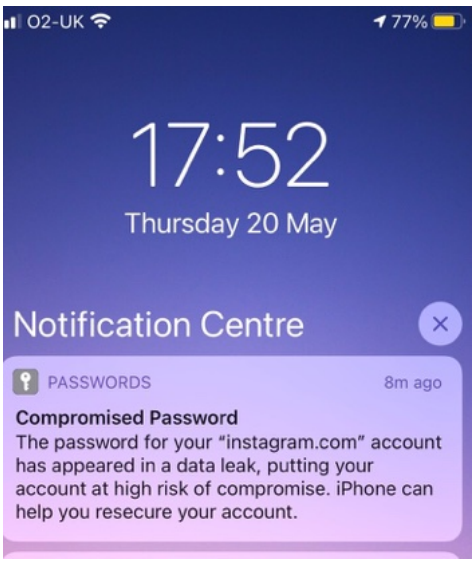
26

2. Using strong passwords

- Avoid commonly used passwords.
- Avoid passwords relating to personal information.
- Avoid passwords that have been breached previously.



27

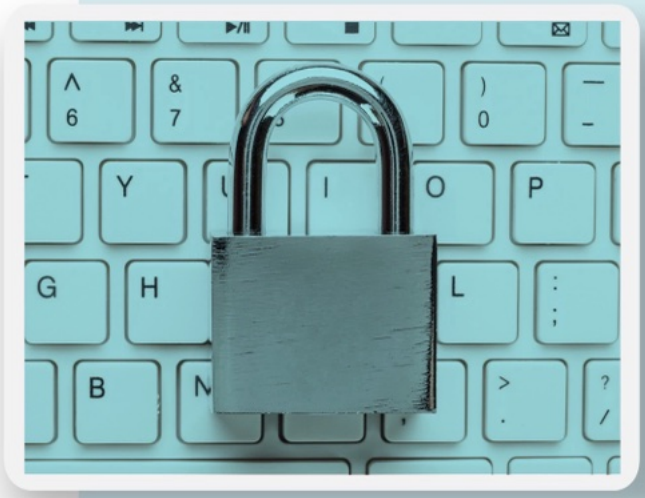


28

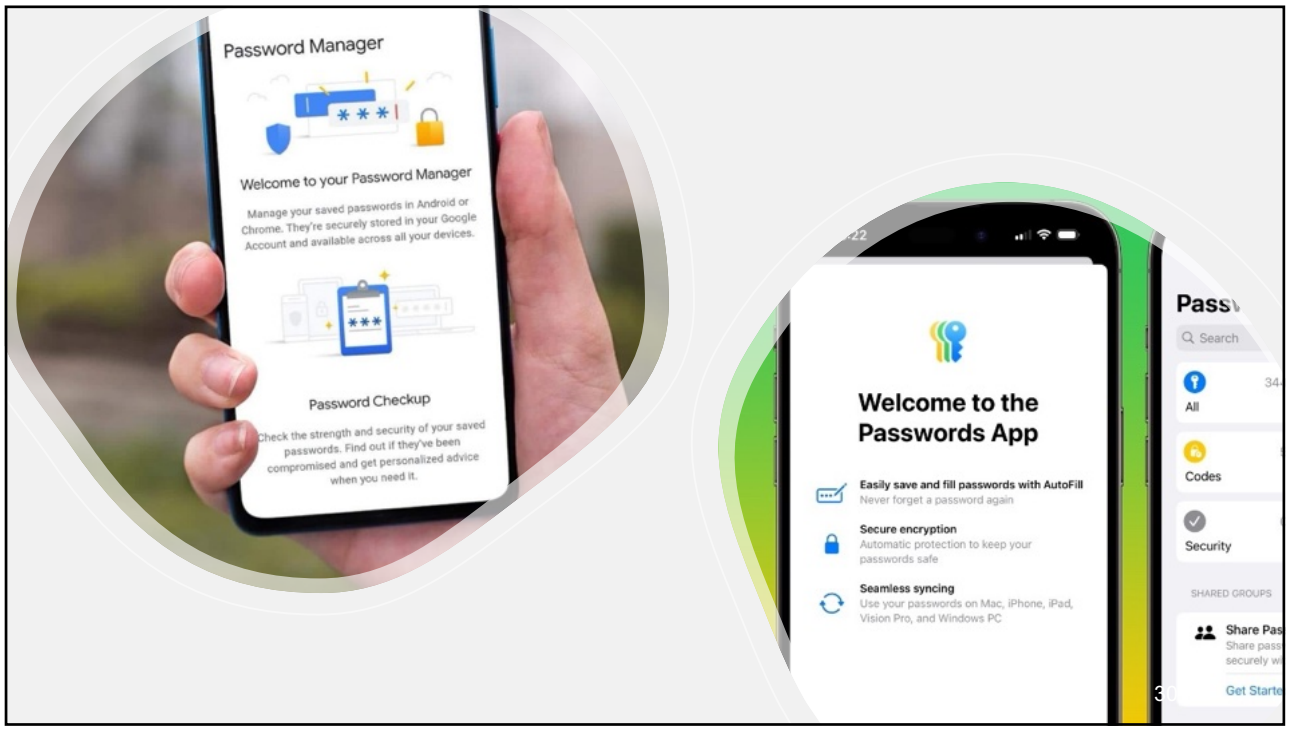
28

2. Using strong passwords

1. Create a strong password for important accounts.
2. Use a separate password for your work account.
3. Where available, switch on two-factor authentication for important accounts.
4. Store passwords securely.



29



30


3. Secure your devices

31


3. Secure your devices
1. School owned devices.
2. Your own devices.
3. Removable storage.

32

3. Secure your devices

1. Do not ignore updates.
2. Only download apps from trustworthy sources.
3. Physically protect your device.
4. If you need to use USB storage, ensure it is encrypted.

33

4. If in doubt call it out

34

4. If in doubt call it out

1. Report any suspicious activity.
2. Report as soon as possible.
3. Don't be afraid to challenge.

35

Summary

Your checklist

Review
Review the privacy settings for your social media, professional networking sites and app accounts.

Know
Know who to report any unusual activity to. If you're not sure, ask your line manager or IT team.

Check
Check your device is set to receive updates automatically.

Set
Set a strong password and switch on two-factor authentication, if available, for your most important accounts.

Remove
Remove any apps that have not been downloaded from official stores.

Check
Check that the password for your work account is unique.

Flag it
If it's not possible to follow security advice, process or policy - flag it to your IT team.

36