EMOTET

Emotet is a trojan virus that spreads through spam emails. The infections arrive with a document file or a link. It persuades people to open or download them by using familiar brand names or by using tempting language. The virus spreads by hijacking your e-mail and then it sends mails to your contacts.

How to protect your computer from emotet?

	2.	3.	4.	5,
Regulary update computer	Don't download SUSPiCiOUS files	Use a strong password	Use two-faktorauthentification	Instal a security program

HOW TO BE SAFE

–

MALWARE

- Don't install things from unsecure websites;

- Put different passwords in the different account;

- Don't enter suspicious links;

- Having a stong anti-virus to protect your phone;

- Don't overuse the suspicious free Wi-Fi;

- Don't answer scam emails.

PHISHING

and how to prevent it

- Don't use personal information in your password or username
- Use different passwords in each account that you have

- Don't chat with strangers on the internet
- If someone asks for your personal information, don't give it to them

- Make sure that your security software is already updated
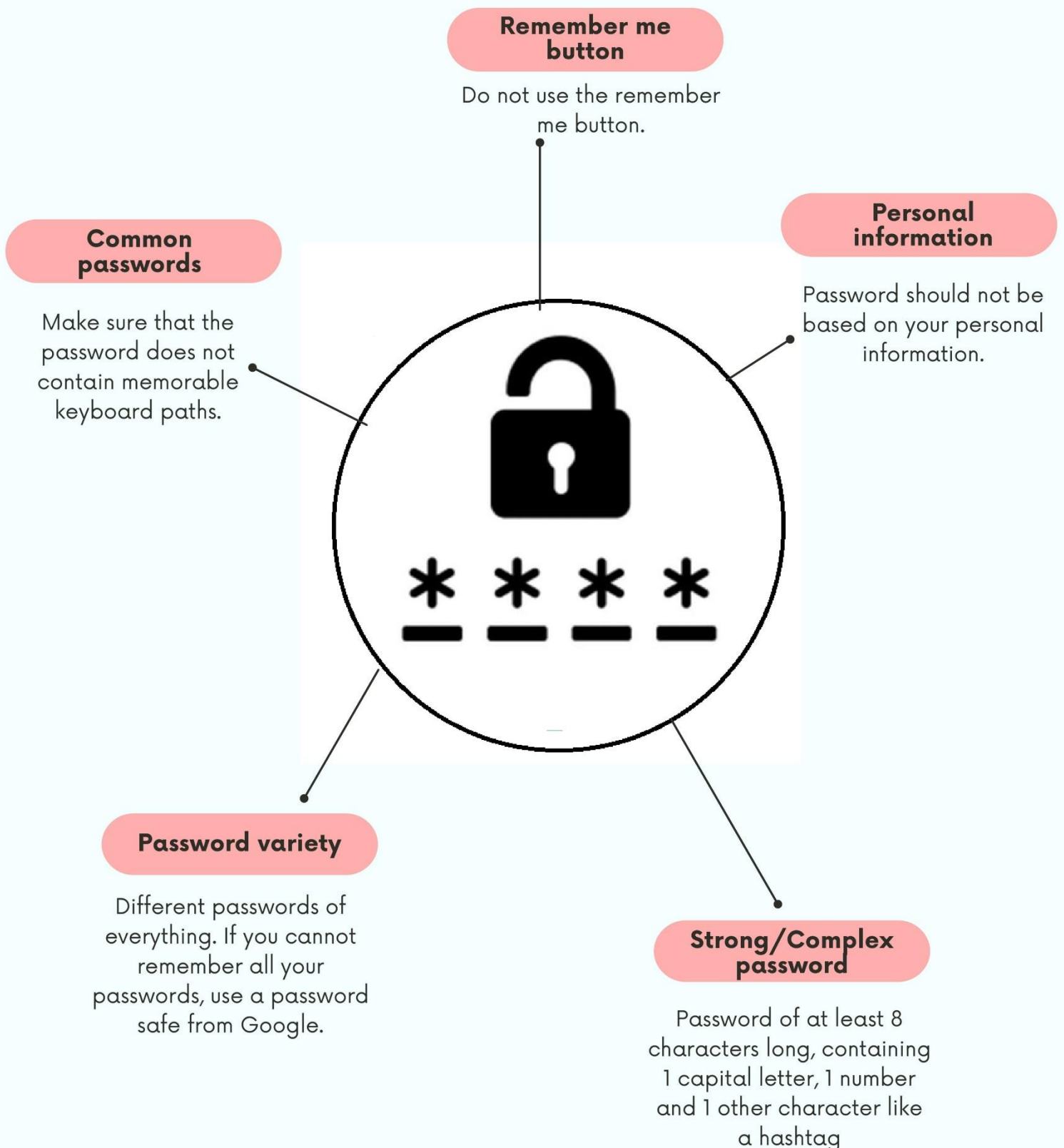- Backup your personal data at a cloud storage like Google Drive

- Don't share your accounts with anybody
- Protect your accounts by using multi-factor authentication (2FA)

- Log into websites that use the *https* protocol
- Always log out when you use a public computer
- Don't do transactions or share personal information using public wifi

PASSWORD ATTACK

Tips to protect your accounts

Remember me button

Do not use the remember me button.

Personal information

Password should not be based on your personal information.

Common passwords

Make sure that the password does not contain memorable keyboard paths.

Password variety

Different passwords of everything. If you cannot remember all your passwords, use a password safe from Google.

Strong/Complex password

Password of at least 8 characters long, containing 1 capital letter, 1 number and 1 other character like a hashtag

FAKE NEWS

1. CHECK THE SOURCE OF THE NEWS
2. DO NOT BELIEVE EVERYTHING YOU SEE ONLINE
3. DO NOT USE SOCIAL MEDIA FOR NEWS
4. READ NEWS ON TRUSTED WEBSITES
5. READ ABOUT THE SAME TOPIC ON DIFFERENT WEBSITES

Made by Group 5