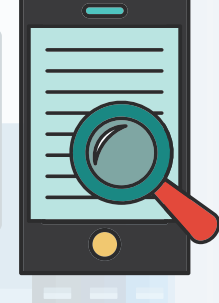# MAKE YOUR HOME A CYBER SAFE STRONGHOLD
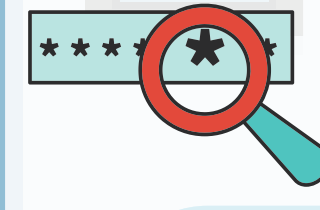
EUROPOL | **EC3** European Cybercrime Centre
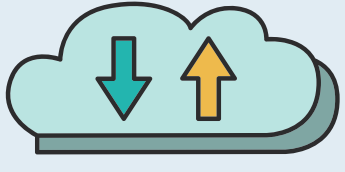
- Wi-Fi: always change the default router password
- Install antivirus software on all devices connected to the internet
- Review your apps' permissions and delete those you don't use
- Choose strong and different passwords for your email and social media accounts
- Back up your data and run regular software updates
- Secure electronic devices with passwords, PIN or biometric information
- Review the privacy settings of your social media accounts

Online shopping safety tips

- Buy from **reliable** online vendors and check individual ratings
- **Think twice**: if an offer sounds too good to be true, it probably is
- **Use credit cards** when shopping online for stronger customer protection
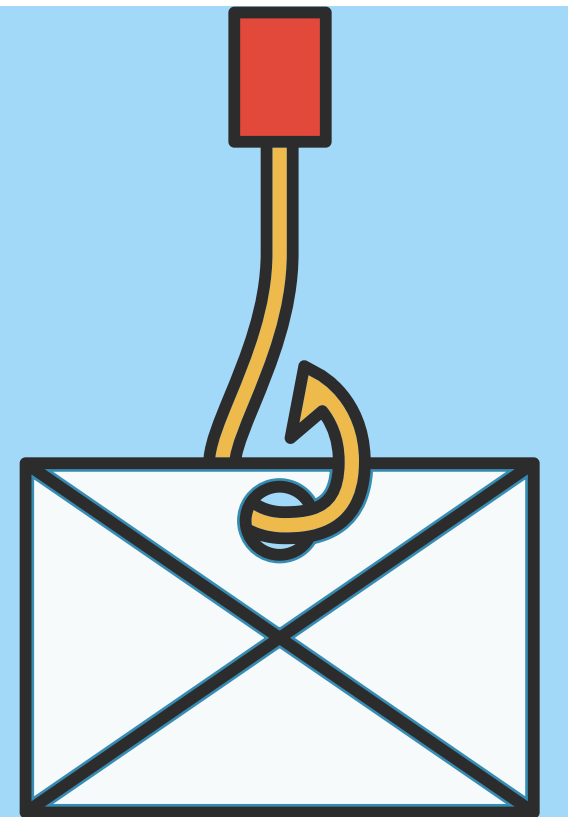- Check your bank account often for **suspicious activity**

Stay alert and <u>don't:</u>

- ⊗ Reply to suspicious messages or calls
- ⊗ Open links and attachments in unsolicited emails and text messages
- ⊗ Share your bank card details or personal financial information
- ⊗ Buy things online that seem to be sold out everywhere else
- ⊗ Send money upfront to someone you don't know
- ⊗ Share news that doesn't come from official sources
- ⊗ Make donations to charities without double-checking their authenticity

EUROPOL

Cyber safety with children

- Change the default factory **password** and keep software up-to-date
- Check the **security** and **privacy** settings of smart toys
- **Talk** to your child about cyber safety. **Listen** to their online experiences and **explain** to them the importance of being just as safe online as offline
- Use **parental controls** to safeguard your child's online activity

REMEMBER
Follow trusted sources for up-to-date factual information. If you become a victim of cybercrime, always report it to your national police.

EUROPOL