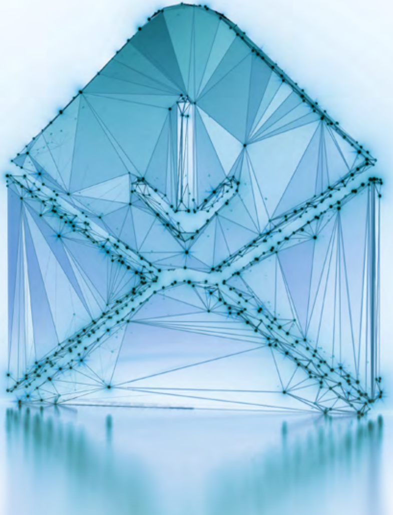
WHICH TYPE OF CYBER-ATTACK IS COMMONLY PERFORMED THROUGH EMAIL?

- A Phishing
- B Smishing
- C Vishing
- D Ransomware



A Phishing

The term 'phishing' is used to describe a social engineering based cyber-attack that arrives mainly by email. Though email phishing is the most popular kind of phishing, other variants of this attacks can arrive by SMS (smishing), phone calls (vishing) or ransomware (digital kidnapping).

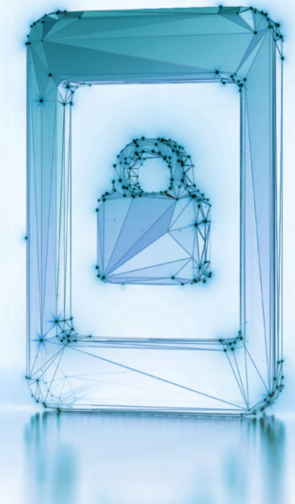
✓

Other choices are incorrect ✗

WHAT KIND OF PASSWORD DO YOU THINK IS THE MOST SECURE FOR ACCOUNTS AND DEVICES?

enisa

- A One word that is meaningful to the user
- B A long list of random words combined with numbers and symbols
- C A series of numbers, such as a telephone number, that is meaningful to the user
- D A short, easy to remember combination of random words and symbols



B A long list of random words combined with numbers and symbols

The longer the password, the less likely it is to be hacked. Security experts suggest using a very long list of random words strung together. Bear in mind that #&5%@>$ is no more difficult than "pancake" for a computer program to decipher, and most hackers don't try to figure out passwords on their own. Instead, they use software to try to steal passwords.

✓

Other choices are incorrect ✗

WHAT IS A GOOD EXAMPLE OF CYBER-HYGIENE PRACTICES?

A Keep a clean desk, without sensitive information visible

B Don’t let the web browser save passwords

C Being alert for suspicious emails, attachments, and hyperlinks

D Don’t use the personal mobile to handle professional information

E All of the above

Ⓐ Ⓑ Ⓒ Ⓓ Ⓔ

All of the above

When it comes to cyber-hygiene, it's about practicing routine cyber-cleaning habits in not just one, but several key cybersecurity areas: avoid phishing and email scams, protect data and devices, browse safely, keep systems updated and connect safely to public Wi-Fi networks. ✓

Other choices are incorrect ✗

YOU HAVE BEEN A VICTIM OF A RANSOMWARE ATTACK. WHAT SHOULD YOU DO FIRST?

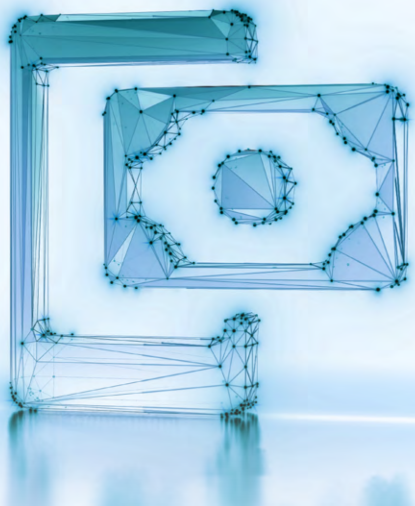
enisa

A Discuss with the attacker to bargain the ransom

B Pay the ransom

C Quarantine affected systems, lock down access to backup systems until after the infection gets removed

D Do nothing

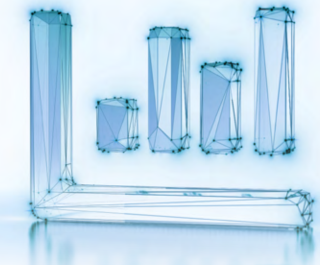


C Quarantine affected systems, lock down access to backup systems until after the infection gets removed

✓

The goal is to remove the ransomware from infected systems, restore systems and files from a legitimate trusted site (ideally from backups), and patch vulnerabilities (if the ransomware has used such an entry vector).

Other choices are incorrect ✗



enisa

- **Europe saw a 234% spike in ransomware attacks in 2021**
- **It was estimated that a ransomware attack occurred every 11 seconds that year**
- **The total cost of ransomware attacks for organisations/ enterprises was an average of €18m in 2021**
- **The average downtime a company experienced in 2021 after a ransomware attack was 23 days**
- **The demanded ransom in Europe grew from €13m in 2019 to €62m in 2021**