kaspersky BRING ON THE FUTURE

Anti-Ransomware Day
May 12th

Anti-ransomware checklist

Conduct backups

Always make fresh backup copies of your files and store them not only on physical devices but in cloud storage for greater reliability. Make sure you can quickly access them in an emergency.

Check backups

Regularly check your backups to make sure all important files are stored, that the backup is not damaged and that it can be restored quickly.

Update everything

Ensure all software, applications, and systems are always up to date. Use a protection solution with vulnerability and patch management features, to help identify yet unpatched vulnerabilities in your network.

Use authentication

Establish the practice of using strong passwords to access corporate services. Use multi-factor authentication for access to remote services.

Educate employees

Explain to all employees that ransomware can easily target them through a phishing email, a shady website or cracked software downloaded from unofficial sources. Ensure staff remain vigilant at all times and check their knowledge with tests.

Protect endpoints and networks

Make sure the right protection is in place on the network perimeter and across all network nodes, including endpoints and servers. Switch on network threat protection functionality to detect and stop encryption if ransomware enters the network. Don't forget to protect embedded devices as ransomware can encrypt them too.

Shield from phishing

Use a protection solution for endpoints and mail servers with anti-phishing capabilities, to decrease the chance of infection through a phishing email.

Audit your networks

Carry out a cybersecurity audit of your networks and remediate any weaknesses discovered in the perimeter or inside the network.

Protect critical roles

Set up default deny mode across applications for those groups of users who have access to the most sensitive data, such as the finance department. This mode ensures an untrusted process can't be launched on a machine.

Do not pay criminals

Ransomware is a criminal offense. If you become a victim, never pay the ransom. It won't guarantee you get your data back but will encourage criminals to continue their business. Instead, report the incident to your local law enforcement agency. Try to find a decryptor on the internet – you will find some available at https://www.nomoreransom.org/en/index.html