TIPS & TACTICS
RANSOMWARE

Quick steps you can take *now* to PROTECT yourself from the threat of ransomware:

1 USE ANTIVIRUS SOFTWARE AT ALL TIMES

Set your software to automatically scan emails and flash drives.

2 KEEP YOUR COMPUTER FULLY PATCHED

Run scheduled checks to keep everything up-to-date.

3 BLOCK ACCESS TO RANSOMWARE SITES

Use security products or services that block access to known ransomware sites.

4 ALLOW ONLY AUTHORIZED APPS

Configure operating systems or use third party software to allow only authorized applications on computers.

5 RESTRICT PERSONALLY-OWNED DEVICES

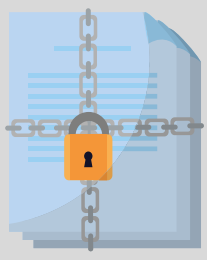
Organizations should restrict or prohibit access to official networks from personally-owned devices.

6 USE STANDARD USER ACCOUNTS

Use standard user accounts vs. accounts with administrative privileges whenever possible.

7 AVOID USING PERSONAL APPS

Avoid using personal applications and websites – like email, chat, and social media – from work computers.



8 BEWARE OF UNKNOWN SOURCES

Don't open files or click on links from unknown sources unless you first run an antivirus scan or look at links carefully.

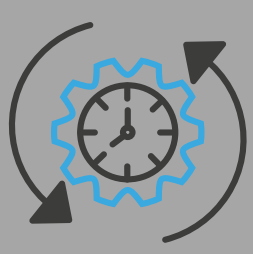
Steps you can take *now* to help you RECOVER from a *future* ransomware attack:

1 MAKE AN INCIDENT RECOVERY PLAN

Develop and implement an incident recovery plan with defined roles and strategies for decision making.

2 BACKUP & RESTORE

Carefully plan, implement, and test a data backup and restoration strategy – and secure and isolate backups of important data.



3 KEEP YOUR CONTACTS

Maintain an up-to-date list of internal and external contacts for ransomware attacks, including law enforcement.

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE