National Institute of Standards and Technology
U.S. Department of Commerce

NIST Releases Tips and Tactics for Dealing With Ransomware

May 13, 2021

Used in cyberattacks that can paralyze organizations, ransomware is malicious software that encrypts a computer system's data and demands payment to restore access. To help organizations protect against ransomware attacks and recover from them if they happen, the National Institute of Standards and Technology (NIST) has published an infographic (https://csrc.nist.gov/CSRC/media/Projects/ransomware-protection-and-response/documents/NIST_Ransomware_Tips_and_Tactics_Infographic.pdf) offering a series of simple tips and tactics.

NIST's advice includes:

- **Use antivirus software at all times —** and make sure it's set up to automatically scan your emails and removable media (e.g., flash drives) for ransomware and other malware.
- **Keep all computers fully patched with security updates.**
- **Use security products or services that block access to known ransomware sites** on the internet.
- **Configure operating systems or use third-party software to allow only authorized applications** to run on computers, thus preventing ransomware from working.
- **Restrict or prohibit use of personally owned devices** on your organization's networks and for telework or remote access unless you're taking extra steps to assure security.

NIST also advises users to follow these tips for their work computers:

- **Use standard user accounts** instead of accounts with administrative privileges whenever possible.
- **Avoid using personal applications and websites,** such as email, chat and social media, on work computers.
- **Avoid opening files, clicking on links, etc. from unknown sources** without first checking them for suspicious content. For example, you can run an antivirus scan on a file, and inspect links carefully.

Unfortunately, even with protective measures in place, eventually a ransomware attack may still succeed. Organizations can prepare for this by taking steps to ensure that their information will not be corrupted or lost, and that normal operations can resume quickly.

NIST recommends that organizations follow these steps to accelerate their recovery:

- **Develop and implement an incident recovery plan** with defined roles and strategies for decision making.
- **Carefully plan, implement and test a data backup and restoration strategy.** It's important not only to have secure backups of all your important data, but also to make sure that backups are kept isolated so ransomware can't readily spread to them.
- **Maintain an up-to-date list of internal and external contacts** for ransomware attacks, including law enforcement.

NIST has also published a more detailed fact sheet (https://csrc.nist.gov/CSRC/media/Projects/ransomware-protection-and-response/documents/NIST_Tips_for_Preparing_for_Ransomware_Attacks.pdf) on how to stay prepared against ransomware attacks. You can find this material and more on ransomware at the NIST (https://csrc.nist.gov/ransomware) and CISA (https://www.cisa.gov/ransomware) websites. These materials were produced by staff members in NIST's Information Technology Laboratory and National Cybersecurity Center of Excellence (https://www.nccoe.nist.gov/).

NIST promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life. NIST is a nonregulatory agency of the U.S. Department of Commerce. To learn more about NIST, visit www.nist.gov (https://www.nist.gov/).

Information technology (https://www.nist.gov/topic-terms/information-technology), Cybersecurity (https://www.nist.gov/topic-terms/cybersecurity) and Cybersecurity education and workforce development (https://www.nist.gov/topic-terms/cybersecurity-education-and-workforce-development)

Media Contact

- Chad Boutin (https://www.nist.gov/people/chad-boutin)
  charles.boutin@nist.gov (https://www.nist.govmailto:charles.boutin@nist.gov)
  (301) 975-4261

Related News

The Phish Scale: NIST-Developed Method Helps IT Staff See Why Users Click on Fraudulent Emails (https://www.nist.gov/news-events/news/2020/09/phish-scale-nist-developed-method-helps-it-staff-see-why-users-click)

Related Links

More Info: Ransomware Protection and Response (https://csrc.nist.gov/projects/ransomware-protection-and-response)
Video: Tips to Help Your Company Protect Against Ransomware Attacks (https://www.nist.gov/video/tips-help-your-company-protect-against-ransomware-attacks)
Infographic: NIST Ransomware Tips and Tactics (https://csrc.nist.gov/CSRC/media/Projects/ransomware-protection-and-response/documents/NIST_Ransomware_Tips_and_Tactics_Infographic.pdf)
Fact Sheet: NIST Tips for Preparing for Ransomware Attacks (https://csrc.nist.gov/CSRC/media/Projects/ransomware-protection-and-response/documents/NIST_Tips_for_Preparing_for_Ransomware_Attacks.pdf)
Released May 13, 2021