Don’t be taken hostage by ransomware.

Ransomware attacks cause downtime, data loss, possible intellectual property theft, and in certain industries a ransomware attack is considered a data breach.

Wouldn’t it be great to have an actionable checklist of what to do when you get hit and how to prevent it in the future? Now you do!

- Ransomware Attack Response Checklist
- Ransomware Prevention Checklist

Don’t be taken hostage by ransomware.
RESPONSE

KnowBe4
Ransomware Attack Response Checklist

STEP 1: Disconnect Everything
☐ a. Unplug computer from network.
☐ b. Turn off any wireless functionality: Wi-Fi, Bluetooth, NFC.

STEP 2: Determine the Scope of the Infection, Check the Following for Signs of Encryption
☐ a. Mapped or shared drives
☐ b. Mapped or shared folders from other computers
☐ c. Network storage devices of any kind
☐ d. External Hard Drives
☐ e. USB storage devices of any kind (USB sticks, memory sticks, attached phones/cameras)
☐ f. Cloud-based storage: DropBox, Google Drive, OneDrive etc.

STEP 3: Determine if data or credentials have been stolen
☐ a. Check logs and DLP software for signs of data leaks.
☐ b. Look for unexpected large archival files (e.g., zip, arc, etc.) containing confidential data that could have been used as staging files.
☐ c. Look for malware, tools, and scripts which could have been used to look for and copy data.
☐ d. Of course, one of the most accurate signs of ransomware data theft is a notice from the involved ransomware gang announcing that your data and/or credentials have been stolen.

STEP 4: Determine Ransomware Strain
☐ a. What strain/type of ransomware? For example: Ryuk, Dharma, SamSam, etc.

STEP 5: Determine Response
Now that you know the scope of the damage as well as the strain of ransomware you are dealing with, you can make a more informed decision as to what your next action will be.

Response 1: If Data or Credentials are Stolen
☐ 1. Determine if ransom should be paid to prevent data or credentials from being released by hackers.
☐ 2. If ransom is to be paid, you can skip steps #1 and #3 of Response 2 from recovery.
Response 2: If Ransom Is Not Paid and You Need to Restore Your Files From Backup

1. Locate your backups
   a. Ensure all files you need are there.
   b. Verify integrity of backups (i.e. media not reading or corrupted files).
   c. Check for Shadow Copies if possible (may not be an option on newer ransomware).
   d. Check for any previous versions of files that may be stored on cloud storage e.g. DropBox, Google Drive, OneDrive.
2. Remove the ransomware from your infected system.
3. Restore your files from backups.
4. Determine infection vector & handle.

Response 3: Try to Decrypt

1. Determine strain and version of the ransomware if possible
2. Locate a decryptor, there may not be one for newer strains. If successful, continue steps...
3. Attach any storage media that contains encrypted files (hard drives, USB sticks etc.)
4. Decrypt files
5. Determine the infection vector & handle

Response 4: Do Nothing (Lose Files)

1. Remove the ransomware
2. Backup your encrypted files for possible future decryption (optional)

Response 5: Negotiate and/or Pay the Ransom

1. If possible, you may attempt to negotiate a lower ransom and/or longer payment period.
2. Determine acceptable payment methods for the strain of ransomware: Bitcoin, Cash Card etc.
3. Obtain payment, likely Bitcoin:
   a. Locate an exchange you wish to purchase a Bitcoin through (time is of the essence).
   b. Set up account/wallet and purchase the Bitcoin.
4. Re-connect your encrypted computer to the internet.
5. Install the TOR browser (optional).
6. Determine the Bitcoin payment address. This is either located in the ransomware screen or on a TOR site that has been set up for this specific ransom case.
7. Pay the ransom: Transfer the Bitcoin to the ransom wallet.
8. Ensure all devices that have encrypted files are connected to your computer.
9. File decryption should begin within 24 hours, but often within just a few hours.
10. Determine infection vector and handle.

STEP 6: Protecting Yourself in the Future

1. Implement Ransomware Prevention Checklist to prevent future attacks.
Ransomware Prevention Checklist

First Line of Defense: Software
1. Ensure you have and are using a firewall.
2. Implement antispam and/or antiphishing. This can be done with software or through dedicated hardware such as SonicWALL or Barracuda devices.
3. Ensure everyone in your organization is using the very latest generation endpoint protection, and/or combined with endpoint protection measures like whitelisting and/or real-time executable blocking.
4. Implement a highly disciplined patch procedure that updates any and all applications and operating system components that have vulnerabilities.
5. Make sure that everyone who works remotely logs in through a VPN.

Second Line of Defense: Backups
1. Implement a backup solution: Software-based, hardware-based, or both.
2. Ensure all possible data you need to access or save is backed up, including mobile/USB storage.
3. Ensure your data is safe, redundant and easily accessible once backed up.
4. Regularly test the recovery function of your backup/restore procedure. Test the data integrity of physical backups and ease-of-recovery for online/software based backups for at least 3 or 4 months in the past. Bad guys lurk in your networks for months and compromise your backups.

Third Line of Defense: Data and Credential Theft Prevention
1. Implement Data Leak Prevention (DLP) tools.
2. Use least-permissive permissions to protect files, folders, and databases.
3. Enable system logs to track data movements.
4. Use network traffic analysis to note any unusual data movements across computers and networks.
5. Encrypt data at rest to prevent easy unauthorized copying.

Fourth and Last Line of Defense: Users
1. Implement new-school security awareness training to educate users on what to look for to prevent criminal applications from being downloaded/executed.
2. Your email filters miss between 5% and 10% of malicious emails, so conduct frequent simulated phishing attacks to inoculate your users against current threats, best practice is at least once a month.

Want to learn more?
Get the FULL 20-page Ransomware Hostage Rescue Manual. This is the most informative and complete Ransomware manual, packed with actionable info that you need to have to prevent infections, and what to do when you are hit with ransomware.