

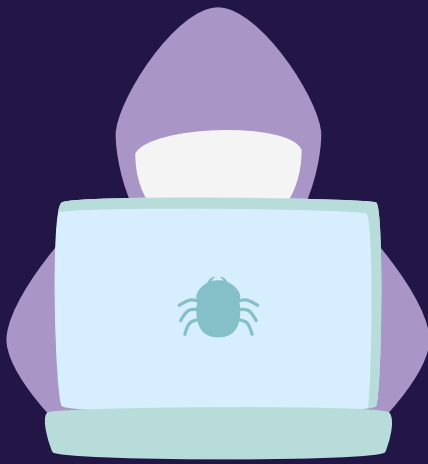
Prevent Ransomware Attacks

- Keep your anti-virus and other malware software updated.
- Back up your data regularly.
- Make sure you only conduct business on secure networks and through legitimate URLs.
- Conduct a risk analysis of your network and security systems and conduct your own hacking attempts to find any security gaps. Patch vulnerabilities as soon as you find them.
- Allow only approved, verified programs and software to run on your computer and networks.



Protect Against Hacking

- ← Be careful about what information you share with organizations online. Don't disclose private information like Social Security numbers, banking numbers, or birth dates unless absolutely necessary.
- ← Use multifactor authentication on all of your accounts.
- ← Monitor your financial statements for irregularities and request a free credit report at annualcreditreport.com.
- ← Don't download or install software or programs if you're not sure of their authenticity.



Avoid Phishing Scams

- Don't click on links or download attachments in messages from people you don't know.
- Double check that websites are legitimate by looking for "https" and the lock icon in the URL address bar.
- Don't share personal or financial data online unless it's absolutely necessary.
- Keep an eye out for changes in your online accounts that may indicate unauthorized access.

