UNDERSTANDING CYBER RISKS

PROTECT YOUR HOME NETWORK TODAY

MIKE O'DONNELL | SAFE COMPUTING | 2026

Email: info@safe-computing.net
Website: https://safe-computing.net

RISKS FOR HOME USERS

The risks for home users are similar in many ways as small businesses face.

WHAT ARE THE RISKS?

The consequences of a cybersecurity attack on your home network can be severe and multifaceted, including:

- **Financial Loss**: Attackers can gain access to bank accounts, credit cards, and online shopping accounts, leading to unauthorized transactions and financial theft. Resolving these issues can be time-consuming and stressful.
- **Identity Theft**: Personal information such as Social Security numbers, driver's license numbers, and addresses can be stolen and used to commit identity theft. This can result in fraudulent accounts being opened in the victim's name, damage to their credit score, and legal complications.
- **Loss of Personal Data**: Important files, photos, and documents can be lost or encrypted by ransomware, making them inaccessible unless a ransom is paid. Even if the ransom is paid, there's no guarantee that the data will be recovered.
- **Privacy Invasion**: Attackers can gain access to personal communications, browsing history, and private files. This invasion of privacy can lead to embarrassment, blackmail, or the leaking of sensitive information.
- **Compromised Devices**: Malware can damage or disable devices, making them unusable. This can require costly repairs or replacements and disrupt daily activities.

- **Social Engineering Attacks**: Scams that allow attackers to use stolen information to trick the victim or their contacts into divulging more information or making financial transactions.
- **Unauthorized Access to Smart Home Devices**: Cybercriminals can take control of smart home devices like security cameras, voice attendants, thermostats, and smart locks.
- **Emotional Distress**: The experience of being targeted by a cybersecurity attack can cause significant stress, anxiety, and a sense of violation. It can also lead to a loss of trust in technology and online services.

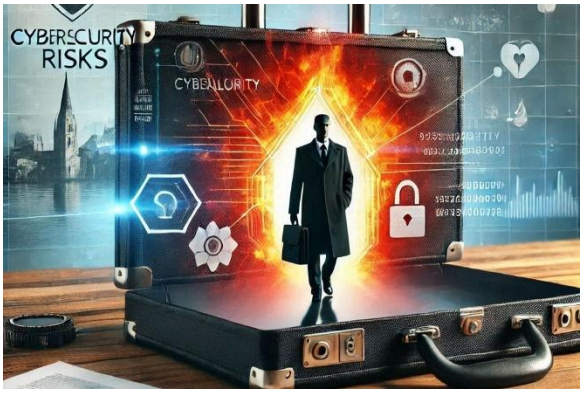
By understanding these potential impacts, home users can take proactive measures to protect their personal information and devices.

Safe Computing
Web: https://safe-computing.net
Email: info@safe-computing.net

WHAT ARE THE SPECIFIC RISKS?

Cyber threat actors utilize a wide array of tools that create risks for your home systems.

- **Phishing** attempts try to trick individuals into revealing sensitive information by posing as a trustworthy entity, often via email.
- **Malware** is malicious software designed to damage, disrupt, or gain unauthorized access to computer systems. Viruses, worms and trojans are types of malwares that can attack your business.
- **Ransomware** encrypts data and demands a ransom for its release.
- **Spyware** is Software that secretly monitors and collects user activity and information without consent.
- **Rootkits** are software tools that enable an attacker to gain undetectable privileged access to a computer.
- **Adware** is software that automatically displays or downloads unsolicited advertising material. Adware is often bundled with other software and can slow down systems or lead to malware infections.



- **Man-in-the-Middle (MitM) Attacks** intercept and alter communications between two parties without their knowledge. This allows the attacker to eavesdrop, steal data and even hijack your computing session. These are often exploited on unencrypted public networks.
- **Zero-Day Exploits** are attacks that exploit previously unknown vulnerabilities in software. There is high potential for damage as there is no immediate defense.
- **Social Engineering** manipulates or tricks individuals into divulging confidential information.

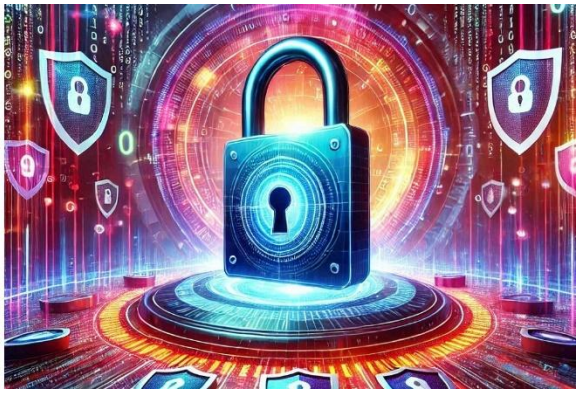
There are mature and efficient processes and tools to prevent or recover from these risks. Studies show that approximately 90% of cybersecurity issues are the result of human error. Cybersecurity awareness training is one of the least expensive and most effective ways to prevent issues.

Safe Computing
Web: https://safe-computing.net
Email: info@safe-computing.net

HOW TO PROTECT YOUR HOME USE

Protecting your small business from cybersecurity threats is crucial. Here are practical steps you can take:

- **Training:** Educate yourself on best practices when accessing the internet.
- **Be Wary of Phishing Scams:** Do not click on links or download attachments from unknown or suspicious emails. Always verify the source before sharing personal information.
- **Use Strong Passwords and Multi-Factor Authentication (MFA):** Implement MFA and encourage the use of complex passwords using a password vault product.
- **Keep Software Updated:** Ensure that your operating system, software, and apps are up to date with the latest security patches.
- **Secure Your Networks:** Use firewalls, encrypt your internet connection, and ensure your Wi-Fi network is secure and hidden.
- **Secure Remote Work:** If you work remotely, use Virtual Private Networks (VPNs), and ensure endpoint security measures are in place.
- **Harden Your Computer:** Enable features that enhance security and privacy and turn off those that create risks.



.

- **Employ the principal of least privilege** as a preventative measure for becoming infected with malware.
- **Stay Informed:** Keep up with the latest cybersecurity threats and best practices.
- **Use Antivirus Software:** Install and regularly update antivirus software on all devices. Configure regular virus cans to remove any malware that was either pre-existing or was able to bypass protections.
- **Backup Your Computer:** Be able to recover your system and data files in the event of a hardware failure or cyber-attack.

Implementing these measures can significantly reduce your risk of falling victim to cyber threats.

Safe Computing
Web: https://safe-computing.net
Email: info@safe-computing.net

SAFE COMPUTING

IS HERE TO HELP

Home users are vulnerable to the same cybersecurity threats that businesses are. Learning by trial and error is a costly and time-consuming way to protect yourself. It does not have to be.

Safe Computing tailors' services in accordance with the Industry Standard Security Frameworks, leveraging the controls that make sense for home users.

Sign up for one of our online seminars on our **training** page. You can also email or call us to learn more about individualized services to cover a broader range of services that include cybersecurity assessment, system hardening, backups and recover, malware removal, VPN, firewall installation and wifi enhancements.

Mike O'Donnell
Phone: 512-228-0411
Email: info@safe-computing.net