

What is Cyber Security?

Cyber Security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

Why is Cyber Security Important?

From the State's perspective, the increasing volume and sophistication of cyber security threats—including phishing scams, data theft, and other online vulnerabilities—demand that we remain vigilant about securing our systems and information.

The average unprotected computer (i.e. does not have proper security controls in place) connected to the Internet can be compromised in moments. Thousands of infected Web pages are being discovered every day. Hundreds of millions of records have been involved in data breaches. New attack methods are launched continuously.

What Are the Types of Cyber Security Threats?

- **Denial-of-service:** Refers to an attack that successfully prevents or impairs the authorized functionality of networks, systems or applications by exhausting resources.
- **Malware, Worms, and Trojan Horses:** These spread by email, instant messaging, malicious websites, and infected non-malicious websites. Some websites will automatically download the malware without the user's knowledge or intervention.
- **"Scareware" – Fake Security Software Warnings:** This type of scam can be particularly profitable for cyber criminals, as many users believe the pop-up warnings telling them their system is infected and are lured into downloading and paying for the special software to "protect" their system.
- **Social Network Attacks:** Social networks can be major sources of attacks because of the volume of users and the amount of personal information that is posted.

What Can We Do To Prevent Against Cyber Security Threats or Attacks?

- **Operating System Updates:** Routinely install validated program updates and patches.
- **Anti-Virus and Anti-Spyware Programs:** Update firewalls, anti-virus, and anti-spyware programs.
- **Passwords:** Use strong passwords (combination of upper and lower case letters, numbers and special characters) and do not share passwords.
- **Communication:** Be cautious about all communications; think before you click.
- **Email:** Do not open email or related attachments from un-trusted sources.
- **System Access:** Allow access to systems and data to only those who need it.
- **Online Transactions:** Only shop at sites for companies you are familiar with and trust.
- **Securing Wireless Networks:** Minimize the risk on your wireless network by enabling encryption and changing the default password.
- **Protecting and Securing Mobile Devices:** secure your portable devices to protect both the device and the information contained on the device. Establish a password and enable screen lock or auto lock on all devices.