PROTECTURO

WELCOME TO YOUR PRIVACY

HOW TO AVOID CYBER ATTACKS

Cyberattacks are not a strictly high-level phenomenon. They strike at all levels of society at any time.

They involve hostile attempts to gain access to or harm a computer system or network infrastructure. Financial loss or the theft of private information, including financial and medical records, can result from cyberattacks. Your reputation and safety are all at risk from these attacks.

Cybersecurity entails preventing, spotting, and responding to cyberattacks that have the potential to have significant negative impacts on people, organizations, the community, and the country.

Cyberattacks can occur in many ways, including:

➢ Accessing your personal computers, mobile phones, gaming systems, and other internet- and Bluetooth-connected devices.
➢ Damaging your financial security, including identity theft.
➢ Blocking your access or deleting your personal information and accounts.
➢ Complicating your employment or business services.
➢ Impacting transportation and the power grid.

Prevention is always the best way to go! Here are some tips:

➢ Don't share too much personal information online. Alter your privacy settings and avoid using location services.
➢ Update your operating system and software programs.
➢ Use capital and lowercase letters, numbers, and special characters to create secure passwords. Use a password manager and two verification methods.
➢ Be wary of any activity that demands immediate action from you, makes an offer that seems too good to be true, or requests personal information. Before you

click, consider. If unsure, don't click.

➢ Use a secure Wi-Fi network and Internet connection to keep your home and/or place of business safe, and update your passwords frequently.

➢ Never divulge passwords or PINs. When possible, employ biometric scanning equipment (e.g. fingerprint scanner or facial recognition).

➢ Regularly check your credit reports and account statements.

➢ Sharing private financial information, such as your credit card number, Social Security number, or bank account number, should be done with caution. Share private information only on safe websites that start with https://. Do not use sites with invalid certificates. Make your connection more secure by using a Virtual Private Network (VPN).

➢ Employ firewalls, anti-virus software, and anti-malware programs to block threats.

➢ Create regular backups of your files in an encrypted file or encrypted file storage device.

➢ Do not click on links in emails or texts that you get from unknown senders. Fraudulent links to websites can be made by scammers.
➢ You should be aware that the government won't approach you about owing money via phone, text, or social media.
➢ Check your account statements and credit reports regularly.
➢ Be cautious about sharing personal financial information, such as your bank account number, Social Security number, or credit card number. Only share personal information on secure sites that begin with https://. Do not use sites with invalid certificates. Use a Virtual Private Network (VPN) that creates a more secure connection.
➢ Use antivirus and anti-malware solutions, and firewalls to block threats.
➢ Back up your files regularly in an encrypted file or encrypted file storage device.
➢ Do not click on links in texts or emails from people you don’t know. Scammers can create fake links to websites.
➢ Remember that the government will not call, text, or contact you via social media about owing money.
➢ Remember that con artists may phone offering work-from-home opportunities, debt consolidation offers, and payback plans for student loans in an effort to capitalize on people's anxieties about their finances.