Catholic Mutual…CARES

CYBER SECURITY BEST PRACTICES FOR WORKING REMOTELY

Advances in technology and the COVID-19 pandemic have paved the way for many workplaces to allow their employees to work completely or partially remote. Unfortunately, remote working and cybersecurity risks go hand in hand.

If you are considering allowing your employees to work remotely, it is important to adopt some basic best practices to protect your devices and business network from cyber liability. Following these guidelines can go a long way in enhancing your overall cyber security position

- **Use a VPN** – A virtual private network (VPN) improves online privacy. It encrypts all the internet traffic, making it unreadable to anyone who may intercept it. Confirm that your employees are using the VPN when working and when accessing workplace information systems.

- **Provide Laptops/Equipment for Work Use Only** – Whenever possible, only use laptops and equipment managed and protected by your workplace. This could be a large investment when developing a remote work environment but using workplace-owned equipment allows your IT department to customize firewalls, add stronger antivirus software, and automatic online backup tools built into business networks. Allowing employees to use a personal home computer could increase the risk of malware invading the computer and accessing personal and work-related information and should be discouraged.

- **Wi-Fi Connection** – Most Wi-Fi systems in homes are secure. When outside the home, (i.e., coffee shop, hotel, etc.), unsecure public wi-fi networks are prime targets for hackers to spy on internet traffic and collect confidential information. Encourage remote employees to work at home and minimize accessing the network on public wi-fi. Have your home wi-fi locked and password protected so that neighbors or other people can't access the network.

- **Choose Strong Passwords** – Using strong passwords is a simple way to prevent cybersecurity issues. Individual passwords should be established for each user. Individuals should not have the same password for work as personal accounts. Unless the employee is on a trusted device, the remember password function should be turned off when logging into the workplace information systems on a personal device.

- **Two-factor Authentication** – Adding a second authentication process for each employee adds an extra layer of protection in preventing the risk of a leak or data breach. The extra step of requiring an email or text confirmation code to the system will reduce access to the data if it was hacked or breached.

- **Backups** – Back-up systems are important to have on employer owned equipment. The system should be backed up regularly to the Cloud. This will save time if a breach occurs. If there were a breach, all the data would be lost without a backup.

- **Install a Firewall** – A firewall is an additional line of defense to prevent data hackers/breachers from entering your system. It creates a barrier between the employee's device and the internet when closing ports to communication. Most employee's devices will have a built-in firewall and if the employee is using a router, a firewall can be enabled on that too.

- **Antivirus Software** – Antivirus software should be installed and fully updated on devices as a next line of defense if threats do get through a firewall. Advanced antivirus software can detect, and block known malware.

- **Encryption** – If employees need to send sensitive information to fellow employees or Church members, encrypted tools should be installed on their device. Many mainstream messaging services come with end-to-end encryption as a default setting or as an option. This will eliminate access by a hacker to sensitive communication. Encryption is also provided with the use of a VPN.

- **Locking Devices** – If employees are working remotely or in a public space, they should ensure that the system is locked or shut down when leaving the device. Password protection should also be in place, which would not allow access to the system until the password is entered.

- **Phishing** – Train employees on how to spot phishing attacks. Employees should be warned of suspicious emails from people they don't know – especially if they are asked to open a link or attachment. Even emails sent from people they know, but asking for unusual things, should be suspect. Every email should be read carefully. Oftentimes, emails that look legitimate may have misspelled words or phrases that can be caught if read.

- **Enable "Find My Device" and/or Remote Wipe** – If your device is lost or stolen, finding the device and securely wiping the device makes it more difficult for hackers to access the data. There are different settings for software programs/equipment that your workplace may be using to set this up.