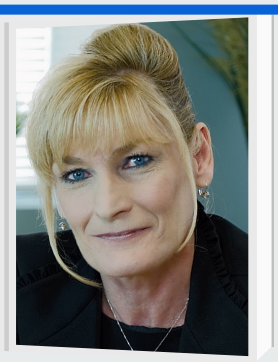
WHAT YOU NEED TO KNOW ABOUT CYBERSECURITY



Suzanne McLaughlin
Executive Vice President, Sales & Marketing
Custom Computer Specialists

Suzanne McLaughlin is Executive Vice President, Sales & Marketing. Suzanne is passionate about technology, but more importantly compassionate in her approach, immediately putting clients at ease. She understands their challenges and is not only their solution provider she is their trusted advisor.

With more than 25 years of technology consulting and management experience, Suzanne focuses on infrastructure design, networking and collaboration technologies. She works closely with Custom's New England education, government and corporate clients to map technology solutions to improve their operational processes and develop strategies to produce high-impact technology solutions.

Suzanne heads up Custom's E-Rate program for the Northeast and has been instrumental in working with school districts and libraries to maximize their E-Rate funding.

Cyber solutions are the future, with remote learning and the growing popularity of the Internet of Things (IoT). Accordingly, focus on the protection and recovery of networks, devices and programs from cyberattacks is no longer a luxury, but a very basic necessity to remain competitive in today's landscape.

Here is a basic overview of cybersecurity.

Things to know:

- Data breaches are intended to access proprietary information, usually for financial gain. These activities can result in damaged corporate reputations, significant downtime and even the cessation of business viability
- Hackers are becoming much more sophisticated, and traditional anti-virus software programs may not be sufficient to prevent attacks
- As more devices and gadgets are connected to networks via IoT, they provide backdoors for hackers to access proprietary data
- Despite the rising prevalence and notoriety of data breaches, they can be prevented. Cybersecurity often relies less on high-end technology than on common sense and solid security practices and protocols, such as:
  - Restricting employee access to sensitive data
  - Employing strong password controls
  - Educating employees on e-mail security
  - Encrypting data
  - Appropriately secure mobile devices – smartphones, tablets
  - Investing in IT professionals with current cybersecurity knowledge and skills

For more information on how we can help protect your district from cyberattacks contact us at 401-775-1286 or smclaughlin@customonline.com

Custom Computer Specialists
Right People. Right Results.®

WHAT YOU NEED TO KNOW ABOUT CYBERSECURITY

Types of Attacks:

- Malware is any type of malicious software utilized to gain unauthorized access to a computer
- Ransomware is a form of malware that locks owners out of their devices/data until a ransom is paid
- Spyware is a form of malware that spies on users in order to acquire sensitive information
- Fileless malware attaches to existing programs running on the computer, thereby embedding inside the computer's memory
- Viruses are malicious programs usually sent as attachments, and which infect devices once downloaded
- Watering holes are when a known website is hacked either directly or via a third-party service hosted on the site. In this way, anyone who visits the site is infected
- Phishing is the act of sending e-mails that trick people into revealing sensitive information
- Spearphishing is related to phishing but is more focused to prey on specific targets by including relevant details about the individual (usually obtained via research), thus luring them to click on the link
- Pharming is the act of directing users to illegitimate websites under the guise of a legitimate link
- Hacking is the act of accessing a network or device without appropriate authorization to do so

Types of Cybersecurity:

- **Network Security:** These are defenses implemented to prevent hackers from gaining access to organizational networks and systems. Examples would be password controls and two-factor authentication
- **Application Security:** This is when software and/or hardware is employed to protect against threats from malicious programs. An example would be antivirus programs
- **Information Security:** This is the protection of data via restricted access or encryption
- **Cloud Security:** These are tools utilized to monitor and protect corporate data stored in the cloud

For more information on how we can help protect your district from cyberattacks contact us at 401-775-1286 or smclaughlin@customonline.com