CYBERSECURITY
in Manufacturing

Has your Facebook page ever been hacked? Has your smart phone been overwhelmed with spam texts? Has your e-mail been compromised?

All of these things that can happen to your personal electronic devices can happen to the computer based devices in your manufacturing plant.

As we move more and more to computer controlled devices, artificial intelligence, and robotics, our manufacturing operations are subject to hacking and electronic attacks.

Ohio Manufacturing Extension Partnership (MEP), Center for Innovative Food Technology (CIFT) and Rhodes State College is offering a series of short courses to help you learn about protecting your manufacturing operation from cyberattack. The series includes 4 sessions listed on the next page.

PROGRAM SESSION

3 month access to the ToolingU classes in CyberSecurity

This is a fully online program.

Self paced program —
Join the class at any time.

Cost: $75 per person
Discounted rate through MEP

Register today! REGISTER

RHODES State College · Ohio Manufacturing Extension Partnership · SINCE 1995 CIFT 25 YEARS OF INNOVATION · TOOLINGU · sme

These courses present a great opportunity for you to familiarize yourself with the threats to your manufacturing systems and develop a strategy to protect critical manufacturing assets.

CYBERSECURITY FOR MANUFACTURING BASICS 101

“Cybersecurity for Manufacturing Basics” covers the foundational concepts of cybersecurity as it relates to the manufacturing sector. As manufacturers adopt Industry 4.0 technology to enhance the digital connectivity of facilities, a fundamental understanding of cybersecurity is becoming more critical to preventing losses due to cyber attacks. The United States government identifies manufacturing as one of the 16 critical U.S. infrastructures. Consequently, ensuring the strength and integrity of this sector is crucial to national safety and security.

Cyber threats generally involve attempts by hackers to utilize malware, such as viruses or digital worms, to disrupt or disable technology or to gain access to systems illegally to obtain sensitive information. Malicious hacking attempts may involve individuals, groups of individuals, or even other nations. This course will help manufacturers and manufacturing personnel understand and identify basic cyber threats.

CYBERSECURITY FOR MANUFACTURING: MALWARE OVERVIEW 102

“Cybersecurity for Manufacturing: Malware Overview” covers different types of malware and how each functions. Manufacturing organizations using Industrial Internet of Things (IIoT) technology and other devices with internet functionality are vulnerable to a range of existing and emerging malware threats. In addition to traditional computer worms and viruses, criminal hackers create other types of malware, such as spyware, Trojans, and ransomware, to attack digital networks. They also employ phishing and other social engineering tactics to manipulate users into performing actions that plant malware onto systems.

Manufacturers should be aware of vulnerabilities associated with all their digital assets and have a basic understanding of the range of tools criminal hackers may use to compromise these assets. After taking this course, users will be able to recognize malware threats. Users will also understand the basic strategies of criminal hackers and ways to defend against them.

CYBERSECURITY FOR MANUFACTURING: HACKING OVERVIEW 201

“Cybersecurity for Manufacturing: Hacking Overview 201” explores the various types of hackers, some common hacking methods, and strategies for defending against hacking. Hackers are generally classified based on their level of skill and their motivations for hacking. Highly skilled criminal hackers develop malware designed to harm digital systems, while less-skilled hackers may look for ways to use existing malware. Skilled ethical hackers work to correct cybersecurity vulnerabilities in digital systems to protect them from criminal hackers.

Criminal hackers present a threat for manufacturers as they can attack digital systems in a variety of ways. This threat grows more complex as manufacturers adopt smart devices enabled by the Industrial Internet of Things (IIoT) and exchange more data across digital networks. After taking this class, users will better understand the cyber threats posed by hackers as well as the tools and strategies to defend against these threats.

CYBERSECURITY FOR MANUFACTURING: WIRELESS NETWORKS 202

“Cybersecurity for Manufacturing: Wireless Networks 202” introduces common wireless technology used in manufacturing and the risks associated with using wireless networks. Common wireless networks used in manufacturing include wireless local area networks (WLANs) and wireless personal area networks (WPANs). Using WLAN technology can expose manufacturers to security risks not associated with wired networks, such as wardriving, piggybacking, and evil twin attack. Additionally, using older WPAN technology or outdated security protocols can allow criminal hackers to easily access digital information through wireless devices.

Manufacturers using wireless technology should understand the risks and employ strategies to protect their wireless networks. After taking this course, users will understand a variety of wireless networking options and their general applications, the risks associated with these networks, and effective ways to make these networks more secure.