OZAUKEE ECONOMIC DEVELOPMENT
FEBRUARY 2020 BLOG

TIPS TO KEEP YOUR TECH SAFE

OZAUKEE
ECONOMIC DEVELOPMENT
Helping Business Grow

Our February Blog focuses on keeping our various types of technology secure. With the accelerated rate that the digital world evolves to make our lives easier, the chance of a security breach of sensitive data increases, and mindful usage becomes ever important. From personal computers and tablets to smartphones, watches, smart speakers, and beyond, these devices are all potentially vulnerable at home and in the workplace. We've asked Joseph Martinez, professor of Information System Security at the school of business at Milwaukee Area Technical College (MATC), for some advice on keeping our technology and data safe.

Lorli Woitas
Ozaukee Economic Development
Marketing & Education Coordinator

Tips to Protect Electronic Sensitive Data

To understand how to protect sensitive data a base understanding on where sensitive data lives is the first step necessary when attempting to secure your environment. For personal data there are two primary categories which include personal identification information (PII), and personal health information (PHI). PHI and PII often exist on the portals or applications that we depend on to run our lives. Technologies such as laptops, smart phones, personal computers (pc)s, and cloud storage sites are all convenient and seen as not under constant attack. In truth PII and PHI personal data has value to both scrupulous and unscrupulous actors (people, programs, corporations and malicious threats).
To protect PII and PHI on any or all of these technologies there are three steps that we can begin with to limit access to our sensate data. Now we must also understand that sensitive data such as PII and PHI is under attack and even the most secure environment has risk of data leakage or exposure. But here are some good steps:

Anti-virus protection

Anti-Virus for smart phones, laptops, and PC's will protect from the effects or goals of virus infestations. Good anti-virus protection should include an antimalware and back up capability that both updates frequently and does not misuse resources on the hosting device.

We are now syncing devices at a higher rate than ever before and not even realizing that our electronics are communicating with one another. Examples include our smart phones syncing with laptops or cloud-based storage services. Home entertainment systems such as Xboxes and PlayStation often sync with much of the mainstream media that we access from all our electronics. Facebook, Netflix and DropBox are all examples on where we can access data from independent technologies placing our source information at risk. To protect these systems, we need to keep up with the latest patches, updates and practice restraint on where and how we access these media types.

Firewall Hardware/Software (FHS)

FHS have configurations that with a small amount of research (YouTube videos, etc..) can be protected in the home to protect our personal environments by placing a barrier to protect our smart televisions, home console systems, Internet of Things (IoT) devices and personal computing devices. These devices include smart TV's, washing machines, refrigerators, web cams, door cams, and home security systems. FHS can provide safe zones for guests/technologies to access the web and not corrupt or pose a risk to your secure environments with the use of access lists or demilitarized zones (DMZ)s. This may sound complicated but there are tutorials both web-based or in print that can guide you down the protective path.

Awareness

We need to be aware of how we access our data, where we access our data and what data has value. An example includes some of our favorite places which include coffee or food establishments that offer free Wi-Fi. Too often it is observed how customers enter these establishments and check work, banking or other sensitive information from devices that can be compromised from the many threats that currently exist out in the wild. These threats include malware, spyware, ransomware, crypto ware and hackers.

In short, basic protections such as anti-virus, firewalls and awareness create the beginnings of an approach to keep your sensitive data safe.

Joseph Martinez, ABD, is a professor of Information System Security (ISS) for the school of business at Milwaukee Area Technical College (MATC). As an ISS professional with 15+ years of experience in both the academic and professional sectors, he has developed the skills and knowledge base on how to protect information resources, both personal and professional.