March, 2017
Volume 12, Issue 3

Common IT Wisdom That Keeps You Secure

MS-ISAC
Multi-State Information Sharing & Analysis Center

From the Desk of Thomas F. Duffy, Chair, MS-ISAC

Day in and day out, employees hear the same things from their IT staff about cybersecurity and safety. Though they may sound like a broken record, there are very important reasons and rationale behind these practices and advice. Keeping safe and secure while connected isn't just about how your system is set up - it is also very much about how you end up using it. Below, we discuss some common IT staff wisdom and provide some background information and the rationale as to why it definitely merits your attention.

Make sure you lock your screen when you are away from your desk.

Screen locking policies exist for a reason. Even if you are leaving for just a few minutes at a time, be sure to lock your screen. Though physical intruders are rare during daytime and in conventionally secured offices, intrusions do occasionally happen. Screen locks also thwart opportunistic insider attacks from other employees that may seek to obtain information or access information beyond what they should normally have. If you don't adhere to a screen locking policy, an attacker can simply walk up and start manipulating or stealing your information without having to even work at getting in to your system. And remember, you are ultimately responsible for everything done under your login!

Don't write down your passwords or user credentials.

The same concept applies here as in establishing a screen lock on your system. On the rare occasion a physical attacker gains access to your desk area, they will immediately look for written passwords and authentication material. Post-it notes, index cards, etc. aren't secure from attackers even if you think they might be out of sight under your keyboard! From looking at your written password, they can get right into your sensitive protected office systems and start stealing data or compromising assets. This risk isn't only from a completely unknown outsider, but could be coming from contractors or internal staff with malicious intent.

Don't re-use your office computer password for other systems and services.

One of the most risky things you can do is use the same password across multiple accounts or systems. Cyber threat actors are constantly stealing login credentials from numerous systems that may be more insecure, like online shopping sites for example. Many times, these

credentials are leaked online for other cyber criminals to also exploit. They then are able to take these stolen credentials and use them to try to access more secure systems, like online banking, or your office systems. If you unfortunately follow this practice of re-using your work password elsewhere, you leave yourself and your organization open to this type of compromise.

Don't install unauthorized software on any office systems.

The installation of unauthorized software can negatively affect your workplace's security posture. This software can include everything from stand-alone programs to plug-ins for your web browser. Not only can this pose a stability issue leading to slower or unreliable system performance, but the installation of unmanaged software can pose a direct security threat either because it may be malicious software itself, or because this is introducing software that is not part of the patch management system in your environment. If this new unauthorized software ends up making you vulnerable to cyber-attacks in the future, but IT isn't aware of it or implementing regular patches or fixes, you leave that avenue open for attackers who easily leverage these known vulnerabilities to compromise systems and potentially steal information.

Don't check your personal email while on office systems.

By checking your personal email on your office computer, you are extending the risk profile of your workplace to include your own personal activities. Attacks that target you as an individual, are now naturally extended to the entire enterprise. Your office email account is carefully managed and secured by policies and the vigilance of your IT team to minimize the risk from suspicious emails, links, and attachments. Once you open your own email account on your office computer, you bypass many of these defenses and render them less effective. If you open that suspicious attachment in your personal email on your office computer, you can infect your system (and eventually many other systems) with malicious software like ransomware that may prevent you or your colleagues from performing their duties.

If you follow these few common pieces of IT wisdom, you will lead a much more secure and productive life in the workplace. Remember, if you are working handling your organization's information, you play a big part in its protection and safety. Let's all work to make it as difficult as possible for attackers to affect our operations in the workplace.

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™