Global Knowledge®

Expert Reference Series of White Papers

Ten Risky Security Behaviors to Avoid: Protect Your Organization

Ten Risky Security Behaviors to Avoid: Protect Your Organization

James Michael Stewart, CISSP, CEHv3-8, CHFIv3-8, Security+, Global Knowledge Instructor

Introduction

You are a problem. You are a risk to your employer. The actions you take and the activities you perform at work, online, and even in your personal life put your employer at risk. You need to know how you are a security risk to the organization and what you can do to reduce or eliminate those risks. In this paper, I discuss ten common risky behaviors that typical workers engage in and what you can do to avoid being the weakest link in your company.

1. Accessing the Spam Folder

It has become fairly standard to have a spam or junk filter operating on your email. Unfortunately, if you can still access messages placed in the spam or junk folders, then no security improvement has been achieved. A security solution would allow you to read the plain-text contents of a spam message but not execute any enclosed scripts, not open any attachments, and not visit any offered hyperlinks. However, this is rarely the case. So, you can avoid being a risk to your organization by staying out of the spam folder. If you have to look in the spam folder, then only look at the list of messages showing the subject lines. If you think there is a valid message in the spam folder, then reach out to your technical support team to inquire about the best procedure to follow to retrieve the message. Keep in mind, you could be wrong and the message really is a problem.

2. Delaying Updates and Patches

Updates and patches are an important part of security management. Most organizations perform testing on newly released updates before pushing them out to the production network. If your environment gives you the option to delay updates, then you should choose to let the updates install immediately. Yes, save and close your work but try not to delay the installation. Within hours of a patch release, hackers have examined the flaws it aims to correct and have written exploits to take advantage of those systems that do not have the update applied. Since your IT staff has already spent days or weeks evaluating new updates, any further delay to installing the updates keeps your system at risk for a longer period of time.

3. Opening Email Attachments

Email remains one of the primary means by which malware is distributed. Through the use of social engineering techniques, hackers craft messages encouraging or tricking you into opening the attachment. Malware can even come from those whom you trust, as their systems may have been compromised and used to send out harmful messages to everyone in their address book. Even well intentioned users might unintentionally send a malware infected file. It is always best to avoid sending or receiving files by email. If you receive an attachment that you believe is valuable and important, send a message back to the sender to confirm they sent the file intentionally. You can also recommend that a file-sharing service be used instead. By not opening attachments, your system will be infected by malware less often.

4. Using Portable Drives

Portable drives are often very convenient, but that convenience comes at a cost. Any portable drive can become infected with malware and then spread that infection to each new machine in which it is connected. Use a file-sharing service instead of a portable drive to avoid spreading malware across multiple systems. Another related problem can occur if you use a personal device to move company documents between business systems. Even after you delete the files off the drive, data remnants may allow the recovery of those files. If you lose the device, anyone with a data recovery tool (such as Pandora Recovery) can regain access to recently deleted files. So, don't use portable drives and you will avoid these two risks.

5. Bypassing Company Firewall Filters

Surfing the Internet from your work computer can be very frustrating, especially when the company implements strict domain, site, and content filters. It is in your best interest to abide by the company restrictions on company equipment. While it may be possible and easy to bypass such filters with tunneling tools, anonymous proxies, and VPN services—you should not do that. Don't be the employee that violates the Acceptable Use and Internet Policy and place the company at risk from malware infection or hacker intrusion. Use either a personal device with your own Internet connection through your wireless carrier or wait until you return home. Playing by the Internet rules of the organization will reduce your risk.

6. Posting Company Information on Social Networks

Many of us use social networks as our primary means of interaction and communication with friends, family, and peers. However, it is easy to forget that much of what occurs on a social network is public, rather than private. Many forget this and assume no one but their online buddies will see their snide remarks or crass statements about their employer. Others even post company private information or proprietary materials to social networks. This is a serious violation of ethics and likely several laws. It's in your best interest to act responsibly on social networks. Don't post anything on a social network that you don't want your boss, co-workers, and family to see. A great rule to follow is: "If you can't say something nice, then don't say anything at all." Posting company secrets to a social network is a fast way to unemployment and possibly a lawsuit. Use social networks to discuss your extraordinary children and your obsession with a TV show. This will reduce the risk you cause your employer.

7. Linking Your Mobile Phone to Company Computers

It may seem silly to forbid you to connect your mobile device, such as a smart phone or tablet, to your work computer; especially when all you are intending to do is charge the device. The problem is that the cable you are using to make that charging connection almost always supports data exchange as well. This causes your mobile device to appear as a storage device to the computer. Thus, malware can infect the company computer from your mobile device and confidential company documents could be copied to your mobile device. These are both serious violations. Even worse issues arise if you use your mobile phone to provide your work computer with an alternate and unfiltered Internet connection. This process is often known as tethering when using a cable but it also can be accomplished via Bluetooth and Wi-Fi. Always limit your work computer's Internet access to that which is provided and secured by the organization. If you must charge your device at work, bring a charging adapter and plug it into a standard power outlet. In fact, keeping such a charger at work and ready to use will reduce the temptation to connect your mobile device to the company equipment.

Another issue related to mobile devices is using them on the company network. If your organization allows personal devices to be connected to the company network, then be sure to read, understand, and follow the company's mobile device policy (often known as the BYOD [bring your own device] policy). If having your personal device on the company network does not give you an advantage to getting your work tasks accomplished, then don't do it. You will be less of a risk to the organization if you keep your personal device away from the company network. If you are able to access your company's email across your wireless provider's Internet link, then often times there are few other benefits to being on the company's internal private network.

So, in either case, you present less of a risk to your organization by not connecting any portable devices to the company equipment or network in any way.

8. Installing Unapproved Software on Your Workstation

If your organization does not have a strict end-user policy in which your account is secured, you may be able to install or launch software that was not provided by the IT staff. If this is the case for your organization, take every precaution to prevent installing or running any application on your work computer until to get approval from the IT staff. The most secure situation would allow only pre-approved applications to execute. This concept (known as whitelisting) ensures that unknown and unapproved software is not allowed to execute. Some organizations only partially implement this restriction by allowing stand-alone software to run, but not allowing software to be installed. This is only a minor security improvement above having no restrictions at all. Whatever your organization's security stance is on this issue, you want to avoid being the user that brings malware or allows hacker instruction through the act of running or installing unapproved software.

9. Accessing File Exchange Services for Non-Work Purposes

For many of us, the Internet connection at work is significantly faster and more reliable compared to our home connection. It is tempting to use the company's Internet link to download large files or a large volume of smaller files so that it saves us time at home. Whether syncing a music library, downloading legally purchased entertainment content, or accessing pirated material, it is always a bad decision to use company equipment for personal activities. First, while you might have the legal right to have possession of the media you purchased on any device you own—the company does not. Copies of your files on the company equipment can be viewed as a copyright and/or license violation. Second, if the content is pirated or the status of the content is unknown, the company's Internet service provider may detect the data transfer and issue copyright violation warnings or disconnect the service completely. Third, you will likely need to connect a personal portable drive to a work computer in order to transfer to your downloaded data so you can bring it home. Just a few points back, I clearly indicated how this is a risk you need to avoid. So, take the high road and don't use the company's Internet link to download personal files.

10. Believing Everything Online Is True

"There's a sucker born every minute" is a phrase likely spoken by David Hannum about P.T. Barnum. The original context was in relation to crowds continuing to pay to see a spectacle even after it was proven to be false and a hoax. This phrase continues to be applicable in relation to content viewed online. Too many people blindly believe anything and everything posted online, especially if they see it through a social network or discover it in relation to an online entity they know. It is important to realize that most of the content on a social network and most other sites is crafted to attract eyeballs and drive wallets, rather than to distribute facts and truth. You need to see the Internet as a source of information, not as a source of fact.

In the last few years we have seen a significant rise in the occurrence of money stealing scams, identity theft, spear phishing attacks, viral marketing campaigns, propaganda, and worse. We have seen the stock market take a nose dive due to a false tweet about the president being injured. We have seen news agencies repeat a tweet for hours as a fact, only later to discover it was a hoax. All too often organizations attempting to make a buck will craft false and misleading information about their product or service.

It is up to you to be skeptical about anything you read online. Take the time to investigate the source of the information. Try to find corroborating or refuting independent sources, both online and offline. If you are unable to determine that something is clearly true, then delay your response and any other investment and avoid re-posting the item. Wait three days and then check again. Don't get caught up in the mob; don't follow along with the masses; don't make any knee-jerk reaction/response. Be patient, be thoughtful, and be reserved. You'll be glad you did.

In relation to your organization, when someone attempts to contact you outside of the normal means used at work, be cautious. If you normally talk with a client over the phone but they are now using your personal email or posting to your Facebook page, don't immediately believe it is the real entity. If asked to give details of an order, a product, a press release, an element of research and development, or whatever—if it is not your job/department/responsibility and you are unable to establish solid verification of their identity—then stop responding to the unknown outsider. Report the incident to your security staff and ask for instructions on how to proceed. Most companies have a communications policy, so be sure to read, understand, and follow that policy. Be vigilant and don't believe everything you see online. All of these tips will help you from bringing larger risks to bear against your organization.

Conclusion

Most of the time, the reason a worker is a risk to the organization is because they don't know the company rules and thus are unable to follow them. It is always your responsibility to read and understand all of the policies and procedures relevant to you and your job. Company security policies were written to protect the company and their employees. Thus, knowing these policies and abiding by those guidelines will keep the company more secure and reduce the chance that a security violation will be traced back to you.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

- Cybersecurity Foundations
- CompTIA Advanced Security Practitioner (CASP) Prep Course
- CISSP Prep Course
- Social Media Security Professional (SMSP) Prep Course

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

James Michael Stewart has been working with computers and technology for over thirty years. His work focuses on security, certification, and various operating systems. Recently, Michael has been teaching job skill and certification courses, such as CISSP, ethical hacking/penetration testing, computer forensics, and Security+. He is the primary author of *CISSP Study Guide, 6th Edition*; Co*mpTIA Security+ Review Guide: SY0-401, Security+ Review Guide, 2nd Edition (SY0-301)*; *CompTIA Security+ Training Kit (Exam SY0-301)*; and *Network Security, Firewalls, and VPNs*.