Global Knowledge®

Expert Reference Series of White Papers

10 Things Security Experts Wish End Users Knew

10 Things Security Experts Wish End Users Knew

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

Introduction

Security is an essential business operation more than ever before. However, without end users improving their knowledge base and behaviors, the technology that an organization deploys is insufficient. In this white paper, I discuss ten things that security experts wish end users knew. The more users understand about risk and consequence, the more likely they will adjust their behavior and assist with supporting security. These concepts are concerns that security experts want you to know.

Software Updates Should Be Installed Promptly

Later in this paper I mention the issue that new is not necessarily secure. However, that does not mean that new is less secure or that old is securer. Security experts want you to know that software updates should be installed promptly, *but not blindly*. Just because a vendor has released an update does not mean it should be taken as a sign to install the update instantaneously. The new code you would be adding to your system could be flawed or could cause unexpected results in your system that the vendor did not predict. Thus, under no circumstances should you install new updates before testing them and learning from others.

Always test new updates on dedicated test systems. Then, work through all major work tasks to ensure that the changes to the lab systems do not interfere. Next, review any comments, reviews, or feedback available about the update from others. You are unlikely the first person to consider installing a new update. Thus, learning from the experiences of others can save you from downtime and repair headaches. Once you are satisfied that an update is reasonably safe and appropriate to install, take one more precaution: back up your target systems. With a system backup, if the worst happens and the update process fails, the update corrupts your system, or new unforeseen consequences arise, you have a path to restore your environment back to a functional state.

To be even clearer, software updates should be installed promptly without skipping testing. In most cases, running the most current and complete set of code available will provide you with the most security form of the product. When updates are delayed or skipped, flaws will remain in your environment, which can be discovered and exploited by attackers.

Account Authentication Strength

A regular occurrence in technology news is a story about yet another person's account being hacked through the use of a password compromise attack. What is so frustrating about many of these stories is when the victim's password is revealed to be something short, simple, and easy to remember. What security experts want you to know is that a password can be made securer with just a few basic steps: (For a complete discussion of secure passwords, please read my white paper entitled "10 Steps to Better, Stronger Passwords.")

1. Make your password longer. Fifteen characters is a reasonably secure length, assuming you follow other good password practices.
2. Never use a single character type. Use three or four character types: uppercase, lowercase, numbers, and when possible, symbols.

3. Do not reuse the same or a variation of a password. *Ever*. Not on the same site and not on different sites.

You can further improve your online password security through the use of a credential manager, such as LastPass, KeePass, 1Password, or Dashlane. These will enable you to generate random passwords with the maximum length allowed on each and every site, while securely storing those passwords for you.

It is also important to use the two-step or two-factor authentication offerings from an online site. A growing number of websites now support multi-step authentication. You should enable this feature. While it initially will be cumbersome, once you become familiar with the process, it will make your online account significantly securer.

Once you have secured your online accounts to stronger passwords and/or multi-factor authentication (where available), you can rest easier knowing that the media haranguing about another account compromise will be even less likely to actually affect you.

All Software Has Flaws

In the highly competitive marketplace of computer software and related technologies, you often hear marketing and advertising messages claiming their product is secure or at least securer than some other product. Often these product slingers want you to believe that, just by installing their solution, all your security worries will disappear. What security experts want you to know is that there are no perfectly secure systems and all software has flaws.

Software is written by humans (at least for the most part). Humans are imperfect and they regularly make mistakes. When those humans are writing software code, they are inevitably going to make mistakes as they type the code. Some of those mistakes will be typos, others will be logical flaws, while still others will be errors of omission or oversight (such as failing to prevent an unwanted event rather than just planning for only expected ones). As a software product grows larger and as more programmers are involved in its development, the likelihood of errors making their way into the final version is almost guaranteed.

A modern server operating system can include over one hundred million lines of code written by hundreds of programmers. While testing, auditing, and reviewing are often performed, it is just not feasible to track down and correct every single issue. For a software product to be perfectly secure, all errors and logic flaws need to be discovered and removed. For a software product to be vulnerable, only a single error or oversight needs to be left in the code. Attackers only need a single vulnerability to exploit a system. At some point, the process of debugging code becomes too expensive. Once a vendor decides they have reached the point of exhausting the cost-effectiveness of their debugging process, they hope that they have discovered and resolved the easy-to-exploit issues and left behind only those that are difficult to detect and exploit. However, we, as the software-using public, know this process is not perfect as we are constantly installing updates and still experiencing breaches.

An important takeaway from this issue that all software has flaws is to use a multi-layered defense strategy. Rather than using a single product or even multiple products from the same vendor, we should use multiple products from multiple vendors to have overlapping security protections. This defense-in-depth approach will minimize the chance that a single flaw in a single product will result in the compromise of the entire organization. Instead, the attackers will need to find a complex gauntlet of flaws, which in turn makes it more likely their attack efforts will be detected and thwarted long before they are ultimately successful.

Every Internet Interaction Should Be Encrypted

In a world where you now know that the NSA and other international government entities are actively

monitoring Internet activity, and where criminal organizations are lurking to find new victims, the fact that we will perform most of our online activity in clear view form is absurd. Security experts want you to know that you need every Internet interaction to be encrypted. The only way to combat Internet eavesdropping is to encrypt your packets.

Having every communication over the Internet be encrypted is not automatic or guaranteed. But with a few simple steps, you can encrypt a majority of your online communications. First, start using Chrome, Firefox, or Opera as your Web browser with the plugin from Electronic Frontier Foundation's (EFF) HTTPS Everywhere (https://www.eff.org/Https-Everywhere). This browser extension converts every URL you click or type from a plain-text HTTP link into one requesting the TLS secured HTTPS version. Only if the server is unable to offer an HTTPS response will you fail back to standard plain-text HTTP.

Second, for every other service you use, such as email, file transfer, or even newsgroups (USENET), use the TLS encrypted connection option provided by the server. This usually requires that you have a software client on your system rather than using the web interface for these other forms of online communication. When a service offers secured connection options, they typically include a how-to guide that helps you through the configuration process.

Third, use a VPN. There are a wide range of free and paid VPN services online these days. Find one you like and use it. Especially, when using wireless connections outside of your own home or office. That includes Wi-Fi networks as well as mobile network operator networks. Setup the VPN to operate on your home systems, your notebook/laptop, tablet, and smart phone. Use it always.

For more discussion on this issue and for VPN suggestions, please see my other white papers: "How to Secure Online Activities" and "Why and How You Should Use a VPN."

The Cloud Is Not a Security Silver Bullet

Cloud services are the new technology addiction for companies small to large. Almost every major product vendor is offering cloud services or cloud extensions or cloud access or cloud enhancements. Security experts want you to know that the cloud is not a security silver bullet. Having another organization perform a service for you or offer a product to you that you could do yourself internally might be a good idea. Other organizations may be better at offering technical support, running websites, or performing accounting. Leveraging the skills and expertise of others is an important part of the business world today. It can be cost-effective and efficient. But it is not necessarily securer.

It is important to keep in mind the truth behind the marketing phrase "the cloud" or "cloud services." There is no cloud. There is no floating collection of magical Internet architecture hanging majestically in the stratosphere just waiting to offer you newfangled capabilities and throughput. Instead, the cloud is just remote virtualization. In other words, the cloud is a collection of computer systems located in some warehouse which run virtualization solutions in order to host numerous operating systems and relevant software products. The resources and capabilities these warehoused computers support are then sold off to customers in a remote-access / remote-use concept under the label of "cloud services."

Thus, being a cloud solution does not automatically make it a securer option than what you could have created inside your own building. You are dependent upon the cloud vendors' security design, expertise, and experience. If they did a poor job of implementing logical and physical security, then that can directly and negatively affect your data and communications hosted on their systems. Always thoroughly investigate a cloud provider's track record and security policy before placing the core of your organization at risk.

A Hacker Is Not a Criminal, Criminals Are Criminals

It has become a standard and regularly occurring news story to discuss attacks and security breaches of both individuals and organizations that are attributed to hackers. Security experts want you to know that a hacker is not a criminal—*criminals* are criminals.

A hacker is anyone who invests time and effort into thoroughly understanding a system, solution, or device. A hacker often disassembles and reassembles, while making adjustments and modifications to learn how the system reacts or changes based on those changes. A hacker can be thought of as an enthusiast. A hacker might focus on learning and understanding, improving and adjusting, or finding flaws and holes that need addressing.

The problem is when someone uses the term *hacker* to always mean a criminal or malicious hacker. Without proper context and explanation, the term *hacker* can cause confusion as well as place blame on those who are innocent. With the terms *criminal* and *attacker*, it is direct and obvious that the individual being referred to is violating a company policy and/or a law. But with *hacker*, that is not necessarily obvious. If people who consider themselves hackers violate polices and the law, then they have become a criminal. However, if they stay within the confines of company policy and legal restrictions, then they are still just hackers. It is good practice to use a distinct qualifier when intending to use the term *hacker* for the purposes of referring to a criminal, for example an unauthorized hacker, unethical hacker, malicious hacker, or criminal hacker.

Ultimately, hackers—especially the ethical ones, not just the criminal ones—help make technology securer. Just because hackers know how to bypass security or break a system does not mean they intend to do so nor that they have the intention of causing harm. Many security researchers are effectively hackers. Most product vendors have code reviewers, auditors, and internal testers, all of which are a form of hackers. By discovering and understanding the flaws and mistakes in technology, those concerns can be patched or otherwise addressed. Hackers have the ability to think in odd and unexpected ways: they don't have to follow the logic of the computer program; they can make unexpected assumptions or take unpredictable actions. This freedom to examine technology without being forced to abide by its rules helps hackers understand and ultimately improve that technology.

New Is Not Necessarily Secure

New software solutions and hardware products are announced at an ever more fervent pace than before. Many tout their improved reliability, efficiency, and security. But before you spend your money or place your trust in some cutting-edge technology, security experts want you to know that new is not necessarily secure.

The primary issue or concern with new products is that they have not had sufficient testing performed against them. Products that have been in the marketplace for years have had more time to be improved and matured. The new product may have modern features and faster performance, but until the world community has had the opportunity to use, abuse, and hack it, the measure of its security has yet to be taken.

Another aspect of the new is not necessarily secure thinking is that many new products may come pre-infected with malware or have known security holes. For example, in early 2015 it was revealed that a wide range of Lenovo laptop models were "pre-installed" with Superfish (a vulnerable adware product). It is not the case that computer technology becomes less secure over time. Instead, most technologies become securer over time as flaws are discovered and patched. However, once the vendor ends support for a product, it then begins to revert back into a less secure product. For example, public support for Windows XP ended on April 8, 2014, and as new flaws were discovered and exploits created for that OS, the security that Microsoft had integrated into one of its most popular OSes has been degrading ever since that date.
Another nuance in this area relates to the updates to your operating systems, updates for installed applications, and firmware updates for hardware products. In most cases, installing updates promptly is a good security

practice. But what often is overlooked is the essential need to test and evaluate those updates before blindly installing them into a production system. Just because new code is released from a vendor does not guarantee that it will prevent it from introducing new problems to your systems. These problems could interrupt mission critical business tasks or otherwise make your system unusable. Always test new updates on lab systems before installing them onto production equipment.

Computer Attacks Are Rare But Overly Emphasized by the Media

It is easy to be worried and frightened by the worst computer-based criminal attacks, but these attacks are rare. But due to our fight-or-flight-tuned brain, we often over emphasize the unlikely threats and under appreciate the more likely ones. Security experts want you to know that serious computer attacks are rare, but they are over emphasized by the media. Large-scale, massively damaging cybercrimes make for great headlines and attention-grabbing thriller plot lines, but they are very rare in comparison to more mundane exploits.

Most of the issues we should be concerned about are using poor passwords, sharing too openly on social networks, and using plain-text Internet communications. The chance that an attacker will figure out your password, attempt to scam you through email, or eavesdrop on your Internet activities is much more common than having your identity stolen, your retirement accounts being emptied, or your car remotely controlled by an attacker. Plus, with just a few simple actions on your part, you can reduce these common threats. Making stronger passwords and encrypting your Internet connections were covered earlier in this paper. How to be securer online in general online, especially with social networks, is detailed in my white paper "How to Secure Online Activities."

Take steps to reduce your risks on the more common but less dramatic concerns. Then, calm you fears over the massive cyber terrorism plots you hear about from TV, movies, or the media. They are much rarer than you are assuming, and you are an unlikely target. Sorry, but unless you are Warren Buffet, Elon Musk, or Richard Branson, you are just not worth the effort.

There Is More to the Internet than What Google Can Search

Most of us experience the world through a social network and Google. We think that we can learn anything or locate something just by typing in a few keywords for a search. Well, think again. Security experts want you to know that there is more to the Internet that what Google can search.

Google and other search engines use automated spiders or robot website crawlers (both a form of web browsing software) to retrieve information about websites. This information is then stored and indexed in their massive databases. When you perform a search, your keywords are used against this collected dataset to produce the results from which you select and click to traverse to the original source. However, due to website design, authentication requirements, or web crawler restrictions (such as robots.txt), search engines are not able to travel to all possible web pages.

There is also a plethora of other content that is not web based and thus is not able to be indexed by a web-focused site crawler. This non-searchable content is known as the Deep Web. This can include file stores; older Internet communication concepts, such as gopher and USENET; as well as custom content and temporary/temporal content.

While most of what we search for is part of the surface web (i.e., the part of the web that is search engine indexed), often once we click on a search result and dive deeper into the visited site, we may be encountering a part of the Deep Web (i.e., content that is not searchable). To learn more about the Deep Web, a quick surface web search will lead you to numerous articles and how-to guides if you want to go Internet spelunking.

Keep in mind that the Deep Web is a separate concept from that of the Darknet. The Darknet is the collection of computers and services that cannot be accessed (at least not directly) from the Internet as any standard website or service can. Instead, special VPN or anonymization services must be used to gain access. Examples of Darknet Services have included Silkroad and Agora Marketplace. Often these Darknet Services are by invitation only or are exceedingly challenging to locate. One popular access portal to some Darknet Services is Tor (https://www.torproject.org/). However, this does not mean Tor is only used for Darknet access or only questionable purposes—it is just a tool.

Social Engineering Protection and Physical Security Are Just As Important As IT Security

Security is an essential business task. But it also an essential concern for individuals. It should be a company policy, and it also should be a personal lifestyle. Security experts want you to know that social engineering protection and physical security are just as important as IT security. IT security, a.k.a. technical and logical security, are all of the computer hardware and software components that we commonly associate with improving online security, such as encryption, firewalls, authentication, logging, intrusion detection systems, and deep content inspection. However, IT security is just one aspect of organizational and personal security. It is essential not to overlook social engineering protection and physical security. Without all three of these security efforts, your protection infrastructure is incomplete.

Social engineering protection is the attempt to limit or restrict the ease by which an attacker can take advantage of you through cons, scams, or hoaxes. Social engineering attacks can occur in a face-to-face encounter, over the phone, through email, or through text messages. Being aware that such attacks are possible and being on guard against them is the first step to being securer. You need to avoid the trap of automatically trusting everything that is online or electronically delivered to you. All communications can be falsified or spoofed. So, take the effort to verify identity before you depend upon your assumptions.

Physical security is also important. Even with the best IT security money can buy, if your equipment is damaged by a flood or fire or stolen during a facility break-in, your data is still in the hands of attackers. Keeping doors locked, using locked containers or tethers, tracking visitors, and using video recording systems will help improve physical security.

Paying attention to security means sufficiently addressing logical, social, and physical security concerns. Only through a well-designed and balanced effort will a security infrastructure withstand a multitude of attack attempts.

Conclusion

Security is complicated. This has led to the many misconceptions and misunderstandings about security. By paying attention to these ten concerns that security experts want you to know, you can gain knowledge and understanding about security and be securer both at work and in your personal life.

Learn More

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

- Cybersecurity Foundations
- Certified Ethical Hacker v8
- Security+ Prep Course (SY0-401)
- CISSP Certification 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; CompTIA 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.

Michael has also contributed to many other security focused materials including exam preparation guides, practice exams, DVD video instruction, and courseware. In addition, Michael has co-authored numerous books on other security, certification, and administration topics. He has developed certification courseware and training materials as well as presented these materials in the classroom.

Michael holds a variety of certifications, including: CISSP, CEH, CHFI, and Security+. Michael graduated in 1992 from the University of Texas at Austin with a bachelor's degree in philosophy. Despite his degree, his computer knowledge is self-acquired, based on seat-of-the-pants hands-on "street smarts" experience. You can reach Michael by email at michael@impactonline.com.