2015

Personal Computing Security Fundamentals

Glen Sagers  
*Illinois State University, gsagers@ilstu.edu*

Bryan Hosack  
*Illinois State University, bhosack@ilstu.edu*

Follow this and additional works at: [http://aisel.aisnet.org/jmwais](http://aisel.aisnet.org/jmwais)

**Recommended Citation**

Available at: [http://aisel.aisnet.org/jmwais/vol1/iss2/3](http://aisel.aisnet.org/jmwais/vol1/iss2/3)

This material is brought to you by the Journals at AIS Electronic Library (AISeL). It has been accepted for inclusion in Journal of the Midwest Association for Information Systems (JMWAIS) by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Personal Computing Security Fundamentals

Glen Sagers
Illinois State University, gsagers@ilstu.edu

Bryan Hosack
Illinois State University, bhosack@ilstu.edu

Abstract

Information security is at the forefront of timely Information Technology topics, with good reason. It appears that attacks on personal and enterprise computing systems are on the rise. There are many steps to take to create a secure environment, but all are not created equal. The most important steps to take are to choose good passwords, and manage them effectively, and harden devices, then install anti-malware software on them. Encryption of devices and network traffic can protect data at rest and in transit. Networks, especially WiFi, represent a fairly easy attack point for home networks. Turning on Wi-Fi Protected Access II (WPA2), and using a passphrase of at least 20 characters ensures, at least for now, that WiFi can not be compromised. Improving computing security really means education, whether of oneself, one’s employees, or one’s family. Thinking “security first” may seem paranoid, but in today’s world, experience shows that it reflects reality.

Keywords: Information Assurance, Computer Security, Personal Computing Security, Personally Identifiable Information (PII), Network Security, Encryption

Copyright © 2015 by Glen Sagers and Bryan Hosack
1. Introduction

Information Technology professionals must understand the fundamentals of security for data, software and networks. Bruce Schneier (2008) notes “Security is both a feeling and a reality. And they’re not the same.” Managers want the reality of security and the feeling of security. This distinction highlights a vital aspect of both physical and computer security. Actual security can be assessed and calculated. We can calculate the odds of a break-in to a house in a particular neighborhood. The reduction in those odds after installing a burglar alarm can also be calculated. This is, of course, the basis of actuarial science and the insurance industry. You may feel that you are at almost no risk of identity theft, medium risk of dying in a car accident, and high risk of having your home burglarized. As such, you may make a decision to spend a lot of money on an alarm system, but spend very little on firewalls to protect your home network. An objective observer, knowing crime statistics in your neighborhood, may well arrive at the conclusion that you overspent on the security system, and underspent on computer security. Can we be really secure? And, can we feel secure? The answer is a qualified maybe, but we can certainly take effective actions to improve our computing security.

So what represents effective security in a home or Small Office/Home Office (SOHO) environment? This tutorial article focuses on the highest-yield security measures for the SOHO environment. To be sure, many of these same principles apply at the enterprise level, but the reverse is not always true; actions that work at the enterprise level may be difficult to apply on smaller scales. We focus on securing the operating system, malware, network security, wireless security, encryption, backups and disaster recovery, passwords, and information security. A mind map of many of the relationships between these factors is shown in Figure 1. Brief background about each problem will be presented to give context, then practical steps will be presented to address each issue. Finally, although certain products are mentioned throughout this tutorial, that does not necessarily imply specific endorsements, the names given are mostly for example purposes, to point users down the road to finding software that meets their needs.

Figure 1. Fundamentals of personal computing security
2. Improving Password Protection

The first computing security issue to consider is passwords. Improving password security is the lowest-hanging fruit to improve security for most people and organizations. Passwords are everywhere, on portable devices, personal computers, and every website. There are several strategies for managing passwords, some more effective than others.

Security experts advocate using long, strong passwords, and using a unique password for every computer or website. This puts a strain on the memory of us mere mortals; human memory capacity is limited. Many books and websites advocate for at least eight-character passwords, however, the magic length isn’t one-size-fits-all. At this point, many eight-character passwords can be cracked in a matter of hours. As such, we recommend at least ten, and preferably more characters, and using unique passwords for each login. Further, passwords should be changed regularly. To aid users in remembering to do this, we suggest that the user change home and other passwords on the same schedule required by their employer, or every three to six months.

Strong, unique passwords are especially critical for websites and computers where financial information is stored. Online banks should obviously have strong passwords, but don’t forget e-commerce sites, which often save your credit card information for ezier checkout. The same applies to email accounts, which can be used to reset passwords for other sites. An especially well-written account of the dangers of a weak password or security question in the chain of events described by Matt Honan, a writer for WIRED magazine. His Google, Twitter, and Apple accounts were compromised in an hour, and his digital photos, documents, and emails erased from his iPad, iPhone, and MacBook. This was all accomplished because of disparities in how sites check identity, and which bits of information they deem secret. By bouncing between sites and password recovery questions, the attackers were able to get enough information to impersonate him and reset his passwords on one site after another (Honan, 2012).

How can we generate passwords that are both long and strong enough to resist attack, and yet memorable? Words are poor passwords, as so-called “dictionary” attacks can try hundreds of thousands, or even millions, of passwords per minute. The attacker simply has a long list of words, the dictionary, which may include multiple languages, and has a program that tries each in turn. Simply adding numbers or symbols, or ChANGing caSE on a dictionary word does not fix the problem, as many dictionary attacks are hybrid attacks, meaning the program is smart enough to try “mustang”, “1967mustang”, “mustang1967”, and “MusTaNG67”, along with dozens of other permutations. This increases the time to crack the password, but only by a small amount. A long sequence of letters and numbers is much better, but hard to remember. So, to create a memorable, strong password, the following strategy can be employed.

First, think of a sentence that’s around 10 words long. “My dog gets fleas every year in June and scratches all summer” is 12 words. Then, take the first letter of each word, “mDgfeyijasas.” Next, add mixed case, with the result of “mDgfeyijasaS.” If desired, a number, symbol, or both can be added, leaving us a 14-character password “mDgfeyijasaS3!” that’s still fairly memorable, because it’s based on a memorable phrase. As noted above, this modification pattern is not effective on dictionary words, but since the original set of letters isn’t a word, it’s acceptable.

One final note on passwords; length trumps complexity. Adding another character to a password, changing it from ten to eleven characters, for example, increases the time it takes to brute-force attack, or try every possible combination, by a factor of approximately 70. Simply moving from 10 lowercase characters to 10 MixeD CaSE characters only increases the difficulty of brute forcing by about two to three times (NIST, 2009; Rolande, 2012). Many applications, operating systems, and websites now support passphrases, which differ from passwords in that they are sentences, including spaces and punctuation. If supported by the target site or application, the phrase chosen above could be used directly, providing greater security; but at the cost of being hard to type. To generate a safe but memorable passphrase, the method explained in XKCD comic number 936 ([https://xkcd.com#936](https://xkcd.com/936)) works well, it’s simply a matter of stringing unrelated words together (don’t be tempted to cheat and use a well-known phrase; dictionaries for phrases exist, cf., Munroe, 2011).

A password manager is one of the best ways to store passwords. Password managers are simply small databases that encrypt usernames and passwords for websites, computer logins, credit card numbers, and short notes. The encrypted passwords are secured with an especially long and complex master password. Password managers can also generate strong random passwords, so the user doesn’t have to come up with a password for each site. All modern web browsers have password managers built in. Mobile apps such as 1Password, KeePass, and mSecure are another popular way to store passwords that can be taken anywhere. Some mobile password apps can sync to the desktop, and have browser extensions that allow them to automatically fill in password fields. A final option is a web-based password manager, such as LastPass ([https://lastpass.com/](https://lastpass.com/)). This tool can be accessed from anywhere the user has an Internet connection. Password managers are really the only practical way to manage the huge volume of personal passwords each of us must remember.

Two-factor authentication represents better security than passwords alone. Two main methods are used in the consumer...
market. First, the user may be sent a text message containing a one-time password or PIN. The other way uses a one-time password generator in the form of an app installed on a mobile phone or tablet. To log in, the usual username and password is entered, then the user is prompted for the one-time password. This one-time password can only be obtained with something the user has, namely, the mobile device. Even social networking sites and email servers have enabled two-factor authentication. Several regularly updated lists of sites that support two-factor can be found online, and you should enable two-factor wherever possible, cf., Davis, 2015.

A final method of managing computer logins for small companies should be mentioned. Active Directory (AD), a Microsoft product, is often considered the best way to authenticate users in a large enterprise. Setting up AD allows for single sign-on across all computers in the organization, as well as email servers and shared folders and files. It is unlikely that it’s worth setting up AD for home use, both for cost and complexity reasons. But, products like Small Business Server are simple enough for small to medium businesses, and greatly increase security by providing single sign-on, coupled with the ability to audit who has signed on, and from which PC.

Passwords Checklist:

- Use long (at least 10 character), strong passwords, and unique passwords or passphrases on every site.
- Change personal passwords when corporate passwords change, or every three to six months.
- To generate memorable strong passwords, use the first letter of each word in a sentence, then mix case, and add numbers or symbols as desired.
- Use passphrases rather than passwords where possible.
- Use a password manager, perhaps with a printed backup in a safe.
- Use long PINs or passwords on mobile devices.
- Enable two-factor authentication on all websites that support it.

3. Protecting Against Malware

Malware, short for malicious software, is software that tries to damage computers, software, or data. There are many types of malware, most fit into the following categories. Malware represents a danger to both home and business users.

- **Virus** – a small program that, like a biological virus which requires a living cell, needs a host program to run. It attaches to any executable file on the system, and when that program is run, the virus spreads to other executable files.
- **Worm** – several types of worms exist, all share the common trait that unlike viruses, they can spread without a host program.
- **Trojan** – like the Trojan Horse of antiquity, these programs masquerade as a useful utility, but carry a payload that causes harm. The payload may be any of the other types of malware.
- **Spyware** – software that sends private information back to the software’s author. The information sent may be used for targeted ads (see below), but may also send more private information.
- **Adware** – a type of spyware used to deliver ads to the user. Many free apps for phones have adopted this model. In some cases, targeted ads are delivered, often based on browsing history.
- **Ransomware** – software that uses encryption to lock all files on a victim’s system, leaving behind instructions on how to pay a ransom, often several hundred dollars, to decrypt the files. Paying the ransom has shown mixed results. Sometimes, the files have been decrypted after paying the fee, other times, the criminals simply take the money. In either case, paying the ransom simply encourages the criminal behavior. Realistically, if the user does not have backups, they will not be able to recover the files.
- **Botnet software** – botnets are large groups (thousands or tens of thousands) of other people’s computers under the control of one individual, who uses command and control software to have the network of PCs do their bidding. Many botnets are used to send spam, or to perform a type of attack called a Distributed Denial of Service (DDoS), in which all the computers simultaneously try to connect to a specific computer, and overwhelm it with requests. The botnet software is simply the command and control software, which is installed on a victim’s machine.

Malware has evolved over the last decades, becoming increasingly more malevolent. Early malware would try to delete files, especially system files, so that the system wouldn’t boot. Today, while that type of malware is still out there,
most of the newer programs are designed to steal information. Credit card and banking information is an especially profitable target, but any file with private information can be valuable. This information is sent back to the creator of the malware and then sold on underground Internet forums.

Most anti-malware software only detects about 50% of new viruses, but it still needs to be installed (Vigna, 2014). A number of good free programs are available, such as Avast!, AVG Antivirus, BitDefender, and Windows Security Essentials. Due diligence should be exercised with the reputation of either paid or free programs. A good way to check is to read reviews on trusted editorial sites, such as those by various computer magazines. Further, users should realize that free offerings typically come with no support. Under no circumstances should software be downloaded from a source given in a pop-up ad. Such popups often say something like: “A virus has been detected. Click here to download our antivirus software.” The software downloaded from such a popup likely contains malware of its own, and may disable rival antivirus software.

A very common malware vector is a so-called “phishing” attack. Often, phishing occurs via email, or via websites which purport to have free copies of commercial software, or free music. The most effective defense is user education. The basic maxim to follow is “think before you click,” and end-users, including family members, should be trained to carefully evaluate links before clicking. If anything about the content of the email, page, or link looks or feels suspicious, do not click it.

An often-overlooked source of infection is USB memory sticks. While very handy, they can easily spread viruses. When used, a memory stick should be used exclusively on one computer, or at the very most only on trusted computers. Kids bring germs home from school, and electronic “germs” spread similarly, to create major problems.

**Malware Checklist:**

- Install anti-malware software on computers and mobile devices. Many good free options exist for home use.
- Don’t use anti-malware software from popup ads.
- Use special-purpose anti-malware that runs on demand to supplement the basic malware program or clean infections.
- Train users about phishing emails and web pages. If it sounds too good to be true, it probably is.
- Use USB thumb drives only on trusted computers, if at all.

### 4. Improving Operating System and Program Security

Operating systems have a long history of security vulnerabilities. As operating systems have evolved, security of both the software and user files has improved. Still, despite the advances, some work remains to be done by the end user to “harden” the system against intruders and misbehaving applications. Operating systems are not the only programs with flaws, applications need to be updated and patched too.

Once a new computer is purchased, some steps need to be taken to protect it. This process, called hardening, ensures that common vulnerabilities are resolved before the system is put into use. The basic steps are the same for all computers, from home desktops to the largest servers. First, get rid of default users and passwords then create non-administrator accounts for authorized users with strong passwords. Individual accounts should be set up for each user. For home systems, family members, including children, should be taught to use only their own account, if for no other reason than organization of files. Users should also be taught how to select a good password that they can remember, perhaps using the first-letter-of-a-sentence method. Implementing non-administrative accounts may mean some aggravation to parents and network administrators who must authorize each game or application install, running applications as a non-privileged user will prevent many types of malware attacks.

Second, only install software that’s absolutely needed. For a new PC, this may mean uninstalling bundled “bloatware.” The principle here is that an application that is not installed cannot be exploited. This is especially important for servers, but even desktop PCs should have only required programs installed. The next step, and perhaps the most important in hardening a system, is to regularly patch installed software. This includes the operating system (for example, using Microsoft Update), and installed programs. Some applications check for updates automatically, and tools such as Secunia Personal Software Inspector (http://secunia.com/) can automate the process for other programs. Lastly, backups should be configured. More issues related to backups will be discussed below, for now, it’s enough to note that this is a vital step to hardening.
Hardening Checklist:

- Get rid of unneeded default users, and set up individual accounts for all users of the computer, with strong passwords.
- Don’t use administrator accounts for everyday use.
- Install only needed software, and remove any bloatware that came pre-installed with the computer.
- Install patches to the operating system and all installed software.
- Set up automatic updates for the computer or mobile device.
- Configure backup software.

5. Understanding and Using Encryption

Cryptography is the science of keeping communications secret. Early cryptography involved such methods as the Greek scytale, a stick of a known diameter around which a parchment tape was wound in a spiral. The text was then written in the usual fashion, one word or letter at a time along the length of the stick, then the parchment was unwound and the long tape sent to a recipient who had a stick of the same diameter (Wikipedia, Scytale, 2015). The shortfall of this method is obvious; it’s fairly trivial to find the right diameter with very little trial and error. Another classical Greek method, cited by Herodotus, was to shave a slave’s head, tattoo the message into the skin, and wait for the hair to regrow to cover the message (Wikipedia, Histiaeus, 2015). This technically would be called steganography, for “hidden writing”, but the net effect was the same (Wikipedia, Steganography, 2015).

In slightly more recent times, the basics of modern cryptography were born. Julius Caesar used a substitution cipher, in which a letter was substituted for another letter in the plaintext. Most readers probably played with a similar cipher in grade school. Caesar apparently used a three-character shift to communicate with his generals, an example of a three-character right shift is shown below.

Plaintext: Attack the city at dawn
Ciphertext: Dwwdfin wkh flw b dw gdzq

This is obviously easy to decode, to the dismay of many third-graders whose notes were intercepted by a teacher, but again, this was an early type of cipher. In more modern times, ciphers using transposition, that is, moving letters around within the message, or a combination of substitution and transposition in a predetermined pattern have been developed. The best modern ciphers use both transposition and substitution, many thousands of times, to scramble plaintext into ciphertext. This ciphertext may then be transmitted to the intended recipient without fear of interception.

Two main types of encryption are used today, symmetric ciphers and asymmetric ciphers, also known as public key cryptography. In symmetric ciphers, both sender and receiver share the same key, much like if you wanted to give a friend access to your house or car. You would simply copy your key, and give it to them in person. This works well, unless the person is not local, in which case, you would need to securely deliver the key to them; perhaps via a courier. For a house key, this might be acceptable, but what if the key were to a safe or vault? Who could you trust? This is where public key cryptography becomes valuable.

Public key cryptography involves creating pairs of keys, which are mathematically related in such a way that something encrypted by one of the pair can only be decrypted by the other member of the pair. The keys are known as public and private keys, and as the names imply, the public key can be distributed to anyone. That public key can be used by anyone in the world to encrypt a message to the key’s owner. The owner, as the sole possessor of the corresponding private key, is the only party who can decrypt the message. This owner then responds to the original sender, securing the reply with the original sender’s public key, and signing it with his own private key. This signature attests to the ownership of the key, and therefore the identity of the sender. This solves the key distribution problem and provides for non-repudiation, that is, the sender cannot deny having sent the message.

Two very common ciphers in use today are SSL/TLS (SSL for simplicity) and AES. SSL/TLS stands for Secure Sockets Layer and Transport Layer Security, and is the security behind https:// website addresses. The two security suites are work-alikes, and TLS is the successor to SSL, but the two are not interoperable. AES, the Advanced Encryption Standard, is a U.S. Federal standard for encryption; it is currently considered the best standard in encryption. SSL is a public-key cryptography method, AES is symmetric. We discuss SSL in the context of online banking and shopping, and give only brief coverage to AES.

SSL, as a public key encryption method, requires the server operator to generate a public-private keypair. These keys are installed to specific locations on the web server, and used to secure e-commerce and banking transactions or email. Before the installation of the keys, though, another operation needs to take place, signing the certificate. When a new key pair is generated, the server operator sends the public key to a Certificate Authority (CA), such as Verisign or Thawte. The
CA checks the credentials of the server operator, ensuring that the individual or business is really who they claim to be, then signs the public key, which is then called a digital certificate. The CA plays a role analogous to a notary public, attesting to the identity of the operator or business.

When customers want to purchase an item from the website, their web browser requests the digital certificate from the server. The server sends this certificate to the customer’s PC. The customer’s browser then checks the certificate’s signature against a list built into the browser, which contains the credentials of several hundred certificate authorities. Assuming the CA signature is validated, the current date matches the certificate’s valid date range, and that the name of the firm (specifically the domain name) matches the domain name the browser is visiting, the certificate is accepted. The browser then displays a lock icon, and the customer can be assured that they really are visiting the e-commerce site they meant to, and not an imposter’s site. The browser then uses the public key contained in the server certificate to encrypt a temporary symmetric session key that is then transmitted to the website. This symmetric key is used to protect all subsequent communication between the customer and website, until such time as the customer disconnects or closes the browser.

It is worth mentioning that even though the communications are secured, once the customer’s information reaches the server, it is decrypted. If the server operator decides to store credit card records unsecured, they are vulnerable to anyone breaking into that storage, something that the world has seen too much of in recent years. Similarly, the CA validates the credentials of the business to ensure it’s really the business it claims to be; they do not validate business practices. In other words, if “Bob’s Fly-By-Night Electronic Megastore” really is a business, with a correct address, business licenses, and such documents, then the certificate will be signed. Whether “Bob’s” really ships the 97 inch TV’s they advertise for $150 is beyond the scope of the certificate authority’s duties.

User education regarding digital certificates is crucial. Too often, when presented with a browser warning of an invalid security certificate, such as that shown in Figure 2, individuals click through. Doing this opens them to so-called “Man in the Middle” (MITM) attacks, in which an attacker intercepts and can decrypt every message a user sends, and read the message and any replies, including emails, credit cards numbers, and orders. People need to be taught to never accept an invalid security certificate. The risks are simply too great. A good program to force SSL on websites that support it is “HTTPS everywhere” available as a browser extension for the Chrome, Firefox, and Opera browsers (EFF, 2015). While it does not directly protect against invalid certificates, it does try to send users to the secure version of a website, even if they do not expressly request the protocol by typing https://.

AES, as mentioned, is a symmetric key encryption method. If public key encryption solves the key distribution problem so well, why use symmetric keys at all? The answer is simply a question of resources. Public key encryption uses many more CPU cycles than symmetric key encryption. Authenticating the server must be done via public keys, but after that, the bulk of the communication can be done with a much “cheaper” symmetric key that both parties share.

Now that you know the basic mechanics of encryption, what can encryption do for you? The obvious answer is to

---

1 Alternatively, and more commonly, the Diffie-Hellman (DH) key exchange protocol can be used to allow each side to independently arrive at a shared symmetric key. For an excellent video discussion of how DH works, see https://www.youtube.com/watch?v=YEBfamv--do.
make your data confidential, protected from eavesdropping attackers, but the benefits do not stop there. Encrypted data may be protected both while “at rest” and during transmission to another party, and the protection also guards against accidental damage to the data, ensuring integrity. When data is encrypted, the encryption algorithm usually creates a checksum that can be used to ensure the data has not been modified. Second, at least in the case of public key algorithms, the sender can be authenticated. This allows both parties to be sure that they are communicating with the right person.

When and where should encryption be used? Always and Everywhere! Recent data breaches and governmental spying, not restricted to the U.S., should provide adequate evidence of the need for encryption. Two basic data locations to encrypt will be discussed, but they are not all-enshrining. First, data in transit should be encrypted. This means using a Virtual Private Network (VPN). For online shopping, webmail, and banking, the VPN provided by an SSL session is typically adequate. In the face of some SSL attacks such as Heartbleed, Logjam, and Poodle, users are advised to be cautious and exercise due diligence to ensure the servers they connect to aren’t affected by the vulnerabilities. For other tasks, a separate VPN may be desirable. The second place to encrypt data is during storage; this may be subdivided into two types. First, full-disk encryption encrypts every bit of data on the computer’s hard drive, and second, individual files can be selectively encrypted.

Encrypting a file system can be part of hardening a device, as discussed earlier. Mechanisms to accomplish this are built into almost every modern operating system and mobile device, with one notable exception. Before discussing where and how the mechanisms work, it is imperative to note when full-disk encryption DOES NOT work. A device or disk that is powered on, and currently unlocked so that it can be used normally, has already been decrypted. A device that is not powered on is fully protected. The specifics of what’s unlocked, and at what stage of the boot or power-on process decryption occurs is beyond the scope of this tutorial article, but beware that an encrypted, powered-on phone, for example, has no more protection than that provided by the unlock screen; e.g., a four-digit code. So, why use full-disk encryption? To protect against data recovery following a theft or loss of the disk.

Unfortunately for home and some small business users, Windows Home editions do not include full-disk encryption capability. It is only available in the Ultimate and Enterprise editions of Windows 7, the Pro and Enterprise versions of Windows 8 and Windows Server 2008 and later. So, the best that most home users can do is to turn on encryption for individual files. Microsoft Office versions after 2007 can encrypt files, and this should be done to any file which contains personally identifiable information. Passwords for the files cannot be recovered, so they should be stored in an electronic password manager.

Encryption can’t solve every problem, but it should always be used for data in transit, and where possible, stored data should be encrypted. As mentioned, for Home versions of Windows, full-disk encryption is not available, so individual files must be encrypted. For Apple computers, tablets, and phones, and Linux and Android devices, encryption is readily available.

Encryption Checklist:

- Don’t ever click through invalid certificate warnings, and train users to do the same.
- Use full disk encryption where available, especially on mobile devices and notebook computers.
- Use a VPN, especially on untrusted connections, such as public WiFi or hotel connections.
- Encrypt USB drives where possible; this is easiest on a Mac.


Our tour of network security starts at the point where your Internet connection comes into your home. Most home users have a cable, DSL, or fiber optic connection to the Internet. Most also have a dynamic IP address assigned from their Internet Service Provider, with Network Address Translation (NAT) enabled to allow all machines in the home to share one IP address. These two facts represent the first line of defense for a personal connection. With dynamic IP addressing, it becomes harder for an attacker to try to attack a specific person, as the address changes occasionally. More importantly, NAT provides an extremely efficient firewall. The NAT router, usually built into the cable or DSL modem, allows all outgoing connections and blocks all incoming connections by default. This behavior means that no outsider can get into the network directly from the Internet. The best feature of NAT on the modem or router is that it’s automatically configured; the end user does not need to do any configuration to turn it on. To test to be sure that the firewall is truly closed off, a very useful tool is ShieldsUP!, from Gibson Research Corporation (Gibson, 2015). This tool performs a legitimate port scan against your network, for most home users, no ports should appear open. If they do, and you have not explicitly opened that firewall port, further investigation is needed.
The next device that needs investigation is the wireless access point or router. In the past, this has represented a large security hole for the average user, as routers shipped in insecure configurations, and the setup routines were fairly ambiguous. Today, most routers are secure out of the box, but the passphrase may not be. There are two passwords that need to be configured. The first controls login to the router’s administrative web pages. This page is typically accessed by connecting to the router, either wired or wirelessly, and entering the IP address 192.168.0.1 or 192.168.1.1 into the browser’s address bar (exact steps will be found in the manual for your router). The router then prompts for an administrative password. If the default has not been changed, the user is typically “admin” or “administrator”, and the password is either blank, “admin”, “pass”, or “password”. Change this password to something long and complex, and record it. The space provided in the front of the router’s manual is actually a good spot for this; if someone has enough physical access to get the manual, they can probably do more damage than simply stealing the password. Do not lose the password, it will be needed to change settings in the future.

Before discussing the next password to change, a little background is in order on the security settings available. WiFi has three main protocols for security. The first, Wired Equivalent Privacy (WEP) came with the original 802.11 standard in 1999. In 2001, an attack was published that took advantage of a weakness in the way encryption was performed, and subsequently automated tools were developed to crack WEP. The result is that today WEP can be cracked in a matter of seconds by even a non-skilled attacker, and can be done reliably from almost a mile away with specialized antennas (Camp-Winget et al., 2003). Because of this, WEP is thoroughly deprecated and should never be used. The use of the WEP protocol was implicated in the 2007 theft of 45 million debit and credit cards from T.J. Maxx, at that time the largest breach of credit cards in history (Greenemeier, 2007). To summarize: Don’t Use WEP!

To address the shortcomings of WEP, the 802.11 Alliance released two new standards for encryption. The first, WiFi Protected Access (WPA), became available in 2003. This standard was always intended as a stopgap measure (Wikipedia, WEP, 2015). WPA was designed so that devices without suitable processing power, such as older WEP-only access points, could be upgraded via a software update. In 2004, the much more robust WPA2, also known as 802.11i, was released. Subsequently, parts of WPA have been cracked, and it was officially deprecated in the 802.11 standard in 2012. Unfortunately, despite the intentions of the industry to use WPA as a stopgap, WPA is still included as an encryption option in modern production access points, and so it is still sometimes used. But, it shouldn’t be: Don’t use WPA either!

WPA2 is the current best practice standard in wireless security. It has two modes of operation, pre-shared key mode (PSK, a.k.a. personal mode), and enterprise mode. Enterprise mode is the stronger of the two, but requires more hardware and software configuration. As the name implies, it is most often used in enterprise settings, not by home or small office users. In this mode, a user must authenticate via the same username and password they use for all other corporate resources. Assuming that the password chosen is strong, WPA2 networks in enterprise mode may be considered nearly inviolable as of early 2015.

Personal mode is designed for smaller networks that don’t need the complexity of a separate authentication server. To implement this mode, the access point (or wireless router) is configured with a passphrase. This passphrase is then entered into every device that needs to connect to the wireless network. The shared passphrase is used only for initial authentication, that is, to prove the device is authorized to connect. After connecting, the access point shares a separate, unique cryptographic key with the device that is then used to encrypt all traffic. Since that key is unique, even an eavesdropping attacker cannot intercept the conversation. WPA2 PSK can generally be considered almost as strong as WPA2 enterprise, as long as a good passphrase is utilized, e.g., more than about 20 characters.

The next step is to set up WPA2 and choose a good passphrase. Often, the default passphrase is printed on the bottom of the router, but it is not typically very secure. Some are derived from the address of the router, and others simply are short, but regardless, the default should be changed. Once you have logged in to the wireless router, look for a tab across the top, of the router, but it is not typically very secure. Some are derived from the address of the router, and others simply are short, but regardless, the default should be changed. Once you have logged in to the wireless router, look for a tab across the top, or a link on the left side of the page that says something like “wireless settings” or “basic wireless settings”. Then, make sure WPA2 is chosen as the security method in the dropdown box, and set a long, complex passphrase. A WPA2 passphrase can be up to 63 characters long. Various tools exist to generate these long, random passphrases, but honestly, typing the string "${XBBe6MgW7%vLFb}Gk8&&q*Hl*AsbKO[7_5(B/peVs[493#O6B2ocvbVA- &" into the on-screen keyboard on a phone isn’t much fun. Length trumps complexity in passwords and passphrases, so a more manageable strategy is to stick with a plain-English phrase. For example, if you had owned a 1982 Chevy Chevelle at age 16, you might type “My first car was a lime-green 1982 Chevy Chevelle in 1993!!!”. This gives 60 easy-to-type characters, and even if someone knew about that particularly sad chapter in your past, they would be very unlikely to guess that you had used that exact phrasing. Record this passphrase in the user manual also, and then save your changes.

A last issue in WiFi security may be harder to address. The WPS protocol promised to allow one-button secure connections to wireless routers. Unfortunately, the implementation was very flawed, and today a WPS-enabled router can be attacked within a matter of minutes (Viehboeck, 2011). The successful attacker is able to retrieve the WPA2 passphrase, allowing them to connect to the router. To disable this feature, there is often a simple checkbox on the same page as other
basic WiFi settings. Uncheck the box, and save the settings. Then, the hard part is determining whether the setting actually worked. Unfortunately, about half of the routers on the market by 2014 allowed turning WPS off, but the change had no effect. To check, open the Windows wireless network settings tool, and click on the name of your wireless network. If Windows still shows a box saying “You can also connect by pushing the button on the router”, the change was not successful. At this point, your choices are to:

1. Live with the vulnerability, realizing that an attacker (your neighbor’s kid!) could break in within minutes, thanks to online help videos.
2. Check for updated firmware from the router’s vendor (this should be updated anyway, occasionally).
3. Buy a new router, after some research to determine whether the new model has the same issue.

One last WiFi issue that is only a small security flaw is the network name. Many people set the network name, formally known as the Extended Service Set ID (ESSID), to be their name or some other personal information. This makes it easy for an attacker to determine which of the twenty or so networks visible in a neighborhood belongs to the victim. Again, this is not a huge risk, but a better course of action would be to choose a more generic name.

There are two often-recommended fixes for WiFi which are not effective (Mitchell, ND; TP-LINK, 2015). First, many sources recommend hiding your ESSID, or network name. This option is often labeled “turn off SSID broadcast” in the router configuration. However, the WiFi standard requires that the SSID be sent in the clear when connecting, this can be easily read by an attacker. The SSID is not a password, it’s just an identifier; turning it off gives no additional security. The second false security method is Media Access Control (MAC) address filtering. A MAC address is a unique identifier for every device with WiFi (or Ethernet) connectivity. The idea behind MAC filtering is to only allow approved devices on the network. However, like the SSID, a client sends its MAC address in the clear to the router, and it can be cloned. Rather than rely on these false measures, implement WPA2 encryption, with a good (more than 20 character) passphrase.

Firewalls are devices or software that only allow specific traffic to pass across the network. Classical firewalls blocked traffic based on IP addresses or TCP ports. Over the years, firewalls have added capabilities which allow them to filter traffic based on which application is trying to communicate, and based on whether incoming packets are in response to a permitted outgoing connection (SPI firewalls). Modern firewalls add great security, but are often over-trusted. A firewall is not a magic bullet. It can not stop malware already on the computer, and generally can not protect the user against their own mistakes in downloading malicious software. Should a home user install a firewall? The answer is yes, but with caveats. As noted above, most home (and many SOHO) users use NAT connections, which provide extremely good protection for the network from outside attacks.

Host-based firewalls, such as Windows or Mac firewalls, protect individual computers from attackers. Using the principle of defense-in-depth, rather than simply a weakest link, it’s worth turning on the host-based firewall on all computers. If someone gets through the perimeter (network) firewall, they still have a firewall to contend with on each computer. Yes, you’ll be prompted to allow access for applications, especially right after setting it up, but you won’t need to approve apps for long. User training is also important here; people and employees should be trained not to click “approve” on every prompt that pops up. Much like license agreements and SSL certificates, we have been trained to blindly accept everything that we are presented with on a computer screen. Instead, train users to look at the application name, and if it is not something they are familiar with, either ask someone or network administrator who knows, or search the web to find out if it is malware or a legitimate program.

After properly securing the router and firewalls, the remaining devices on most home networks are PCs, tablets, phones, game consoles, and printers, along with set-top boxes for satellite or streaming devices such as Apple TV. Except the PC, most of these devices have very few security settings which can be configured by the end user. Printers, satellite receivers, game consoles and streaming devices typically only need updates applied for best security; usually, this can be done automatically

**Network Checklist:**

- Test your network NAT firewall with ShieldsUp! If any ports are open, and you don’t know why, investigate.
- Enable host-based firewalls on all machines on the network.
- Patch any devices on the network that aren’t PCs, and allow automatic updates for them.

**WiFi Checklist:**

- Change the login password for the router to something secure, and record it in the user manual.
• Set up WPA2 as the encryption method, and set a strong passphrase of at least 20 characters. Record it in the user manual, too. Don’t use WEP or WPA.
• Turn off WPS. Then, check to be sure it’s really off. If not, check for firmware updates for your router, live with the flaw, or buy a new router.
• Set a good network name (ESSID/SSID). Don’t use your name or address, choose something generic.
• Don’t bother with MAC address filtering or hiding the SSID.

7. Providing Backups and Disaster Recovery

There are two kinds of people in the world, those who have never lost data, and those who make backups. Since almost all of us have lost data at one time or another, why haven’t you set up backups for your computer? Many of us would simply say that it is too much effort, and unfortunately, a good backup system takes some time. There are several good strategies that take much of the pain out of the process.

Backup strategies relate to what should be backed up, and how often. There are two main options for each. In terms of what should be backed up, the options are to do image-based backup, which copies the whole hard drive, or to back up only user-generated files. Image-based backup copies are large (the size of the full drive, at least initially), and slow to create. However, when restoration must happen, they are the fastest way to get a system back up and running. The other option, simply backing up the important files and settings is much quicker and smaller in size, but restoration takes longer. In this case, system files and directories are not backed up, the operating system and programs are simply re-installed, then the data is restored from the backup. For home users, full drive backups are typically too large to be manageable, so file-based backups make the most sense.

Both image-based and file-based backups have two further options, to backup each file every time or only files that have changed. The best strategy is probably a hybrid, to back up all files the first time, then only changes. Every week or month, the sum of the changes can be consolidated to a new full backup, and then changes kept for the next week or month. This needs to be done automatically by the software chosen.

The main strategy relating to how often backups occur is to decide how long to keep backups. How many generations of backups should be kept? For a home user, the answer is probably to keep the backups essentially indefinitely, especially things like pictures and video clips. For a business, the answer is a legal matter. Financial records, client records, and so on all have different retention requirements. A firm should clarify these matters before developing a strategy. In terms of how often to back up, the answer really comes down to how much data you can afford to lose. Given the volume of data a home user generates, daily or even weekly backups are probably adequate. For a small business, hourly or every few hours might be a better choice.

The next choice in backups is what medium to use. For a home user, the choice mostly comes down to optical media or USB devices, with optical media decreasing in popularity as fewer machines come with a DVD or Blu-Ray writer. Sizes and cost of hard drives, or even thumb drives, are reasonable, and the process is as simple as plugging in the drive and setting up the backup software.

For a business, tape drives also deserve consideration. Tape drives are fairly slow, and seem like old technology, but have two big advantages. First, the capacity of a tape can be fairly easily matched to the volume of data to back up. Second, tapes are removable storage, and can be sent to offsite storage locations. As discussed next, this can greatly improve the reliability of backups.

Offsite backups add reliability and safety to both home and business computing. If a computer is stolen, or a fire or flood occurs, there’s another copy of valuable data kept somewhere else. For a home user, this can mean buying two drives, backing up to both, then give one to a family member who lives elsewhere, or stash a copy in your office desk. Then, every week, month, or some other period, swap that drive for the one at home that’s getting backups daily. For a business, the same strategy of using two drives or a tape drive can be followed. The business would likely ship the drive or tape to a secure offsite facility, such as one of the numerous document archiving services. Both home and business backup drives or tapes should be encrypted when they’re created for extra security.

The other principal offsite backup method is cloud-based backup. Multiple companies provide online backup services, however, cloud-based sync such as Dropbox, can not be considered backup because when a file is deleted in one location it’s deleted in all. Instead, services such as iDrive, Carbonite, and Mozy, along with many others, provide services that copy files to their servers, and store them for a monthly fee. If disaster strikes, the files can simply be downloaded to a new computer. For relatively small quantities of data, say, a few to twenty gigabytes, these services work well. If a user has hundreds of gigabytes of photos and files, though, the speed of their Internet connection becomes a factor in both backup and recovery.

When choosing a cloud backup provider, be sure to check their reputation, the cost of their services, and whether they offer encryption for security of their files. If encryption is offered (and most do), who controls the keys? Encryption keys can be managed by the backup provider or by the client. If the backup provider controls the keys, they probably would need to
release them for legal requests, such as subpoenas, but it also means that they can recover the keys in case they’re lost. If the user creates and keeps the keys, they have full control over who can access the files, but if they lose the keys, there’s no recourse; the backup is irretrievably lost. Both service-controlled and client-controlled keys are viable options, but make sure you understand your needs and the legal and security implications when choosing.

Once the backup is created, your work is not done. Backups should be tested regularly to ensure that the files are restorable. You may have dozens of backups on external hard drives and in the “cloud” but if the files are corrupted or in some inaccessible form, you need to know about it prior to failure of the original. By occasionally restoring your files to test the integrity of your backups, you are able to ensure that your backup will function accordingly when disaster strikes and you need it most!

**Backup Checklist:**

- Make backups automatic. If backups are manual, they won’t happen. Either pick a program that has built-in scheduling, or use a scheduler such as Windows Task Scheduler to run the program periodically.
- Decide what to back up. For most home users, this will be only their own files and folders, not programs.
- Decide how often to back up. Backups should be conducted often enough to preserve (almost) all changes.
- Decide how long to keep backups. Most individuals will probably keep files indefinitely, firms have legal retention requirements.
- Decide what medium to use. USB drives are usually the best choice, or cloud-based backup.
- If physical media such as a hard drive is used, make two copies and store one offsite; with a family member, in a safe deposit box, or at the office.
- Encrypt backups for added security.
- Restore from backups periodically to test for file integrity and consistency.

---

### 8. Managing Personal Information Security

A colleague of the authors has a poster on his office door issued by one of the three-letter-acronym U.S. government agencies. It shows a trash can with various bits of electronic and printout detritus, and is captioned “Your trash… Could be an Adversary’s treasure. Remember OPSEC: Operations Security”. This highlights an important part of our digital lives; we leave many traces that can be used for identity theft. As individuals or firms, we need to take steps to ensure against leakage of our personal information.

In order to prevent personal information leakage, training is key. Social media sites should not contain posts which give personal details, such as birthdates, addresses, and so on. Further, children should be trained not to post detailed information about where they are going, instead giving only vague information to prevent others from following or stalking them. Train them not to accept all “friend” requests, but limit themselves only to those who they personally know. A little common sense goes a long way toward keeping private information to oneself.

Many of us give out our personal information freely. For example, most shopping rewards programs require a name, address, phone number, and other personal information. What do we get in exchange? A few dollars a year in discounts? A free dessert at our favorite restaurant? Is the sacrifice of our personal information worth these tokens? In some cases, it may be, but stop and think before signing up for yet another loyalty card; what will you receive, and what will it cost in terms of spam emails, marketing phone calls, and similar time wasters? One option is to use throw-away phone numbers or email addresses when signing up for these programs. A good source of disposable emails is mailinator.com, and an unused Google Voice number can be a number that is not technically disposable, but never answered.

A few years ago, one of the authors purchased a computer at a local warehouse club that had been returned, and moved to the clearance section. A handwritten note on the new price tag stated that it was returned because it “runs real slow” (sic). Deciding that this must be a software problem which could be fixed by a simple format and reinstall, the author bought the computer. Before wiping the drive, some forensics were performed. Indeed, the computer did “run real slow”, largely because both Norton and McAfee antivirus were loaded on the computer. Each time any file was accessed or a program launched, both tools scanned the program. Upon removing one of them, the speed increased greatly. Of more interest, however, was a W-2 form in the “My Documents” folder, which contained the name, profession, address, and social security number of the individual, an Army chaplain, to whom it was issued. Apparently, this individual had started their taxes, then grown frustrated with the computer, and returned it, not wiping the drive, or even deleting personal files.

Last year, the same author purchased several hundred USB sticks, hard drives, and digital photo cards from eBay for use in a forensics course. Many personal photos were found, of course, some of which had GPS information embedded in them. Along with the photos, business plans, pay spreadsheets, blueprints, loan documents, school reports, and bank account statements were found on many drives. Some had been formatted, but none had been wiped securely by overwriting the data.
Returning to our trash can, a simple low-tech way to avoid personal information leakage is to shred personal information. A cross-cut shredder is an inexpensive investment, and can add great security against bank statements, bills, and medical records falling into the wrong hands. Old storage devices, such as memory cards and hard drives, as well as CDs or DVDs which contained backups, should be physically destroyed prior to disposal or recycling. If you simply must sell or give away the item, use a program such as Eraser or DBan to securely overwrite the information on the drive with ones, zeros, or random data.

**Personal Information Checklist:**

- Cross-cut shred sensitive documents before recycling or disposal.
- Store paper copies of documents in a lock box or locking file cabinet.
- Destroy storage devices or wipe them securely before recycling, and wipe securely before selling.
- Don’t post personal details on social networking sites, and don’t post detailed travel plans with dates and locations.
- Be selective about what personal information you give out for loyalty or rewards programs. Use disposable emails and/or phone numbers, and never give more than absolutely needed.

9. Final Thoughts on Security Fundamentals

A few useful security measures do not fit in any of the categories above. They are listed here in no particular order.

Both iOS and Android devices have ways to locate lost devices. For Apple, it’s through iCloud, for Android, it’s via the Google Play store, or the Amazon Manage Your Device service. Take a few minutes to familiarize yourself with the process for locating a lost device; it can save valuable minutes if stolen, and make finding it when lost around the house a lot easier too. For laptops and desktops, various recovery packages exist, one notable open-source software package is called Prey. This software can be installed to PCs, tablets, or phones, and perform such actions as locating the device, sounding an alarm, taking pictures of anyone who tries to login too many times with the wrong password, and allows for remote wiping of the device.

Cloud services are a new buzzword, and many of us have one or more cloud storage services, music or movie streaming, and online email accounts. All of these deserve consideration in our overall security posture. For example, if we store files in an online service such as OneDrive, Box, or Dropbox, how secure is that data? Is it encrypted? How strong is the password we use to access it? The first step to securing it is to make sure a good password is chosen, and use two-factor authentication if offered by the site. Then, if encryption isn’t used, decide whether it’s worth keeping your files there. Almost every online storage service has been compromised over the years, and personal data exposed.

Filtering software is a useful option to prevent users from accessing undesirable sites. It may be installed to prevent home or small business users from accessing forbidden sites. This could prevent children from accessing inappropriate material, or to prevent workers from wasting work hours checking sports scores. A full discussion of the options available is beyond the scope of this basic tutorial, but solutions exist that are sized to meet the demands and budgets of home and small office computing. A simple solution for home use is K-9 Web Protection, from BlueCoat Software, which filters objectionable material and can be installed on iOS, Android, Windows, and Mac. One notable open source solution to protect a whole network is Dansguardian (http://dansguardian.org/); setup is not the easiest process, but a good IT professional should be able to handle the task.

Moving forward you should be constantly aware of the-ever shifting security landscape. If you only take two things away from this tutorial article, we would challenge you to have:

1) Heightened Awareness – Be aware of your organizational or personal security strengths and weaknesses in all aspects. Try to objectively evaluate the true degree of risk to your systems and data, and realize that people can feel secure even when they are not.

2) Embrace Change – Revisit your security and recovery plans occasionally, and keep up with developments in the security field.

Can we correctly evaluate the level of risk in our computing lives, and fix things that make us less secure? **Yes.** Whether we can correctly match our feelings of security with the reality of security is less certain, but when we evaluate the risks correctly, we are closer to reality. Security is always a trade-off, usually trading some ease of use for better security. A normal user can have nearly perfect security by encrypting a hard drive on the PC, then turning the computer off, disconnecting it from the network, and never powering it on again. However, this also sacrifices all usability. The goal of information assurance is mitigating risk to a reasonable level for a reasonable cost, whether in dollars or usability.

Home and business users alike can benefit from basic security measures, which can be implemented by almost anyone.
with computer experience. Chief among the easy fixes for most users are to implement long, strong passwords and passphrases, and use unique passwords for each website. To help manage the proliferation of passwords created by this strategy, use a password manager. Great passwords are especially vital on financial sites and cloud storage sites, which contain the most personal information. For the ultimate in authentication protection, two-factor authentication should be used, but it’s not available on every website yet.

To protect the hardware and operating system of a single PC or portable device, two main sets of actions can be taken. First, the device should be hardened. The basic steps of hardening consist of getting rid of unneeded software and user accounts, and keeping software, whether the operating system or applications, up to date. Automatic backups are the next step in protecting data, and should be done as part of the hardening steps. The three key decisions in configuring backups are to decide what should be backed up, how often it should occur, and how long the backups should be kept. After these steps are done, the second action is to install anti-malware software. Many good free and paid programs are available.

Encryption is the key to protecting data at rest and in transit. Full-disk encryption is especially important on portable devices and USB drives as they represent loss and theft targets. Unfortunately, this is difficult for Windows Home Edition users, so sensitive individual files should be encrypted by the application which produces them. Full disk encryption protects data in storage on the device, at least as long as the device is powered off when found. For protecting data in transit, the primary tool today is SSL/TLS. SSL certificates provide both strong encryption and strong assurance that the site being visited is really the site it claims to be. To provide such assurances, it is imperative that users be trained NOT to click past invalid security certificates. However, when traffic other than web browsing needs to be protected, it’s time to turn to more formal VPN configurations, such as IPSec or OpenVPN servers, which protect all traffic from the user to a site, or a central to a branch office. Encryption doesn’t solve all security problems, but implementing it is vital.

To protect networks, a first step is a firewall. While firewalls are too often trusted as magic bullets, they play a vital role in keeping attackers out of a network. Luckily for home users, the NAT technology used to allow multiple internal devices to share a single IP addresses acts as a great firewall. Home users likely don’t need another network firewall. Individual machines should have host-based firewalls, such as Windows or Mac firewall, enabled. The other major component in most SOHO networks is the wireless router. Turning on strong encryption, in the form of the WPA2 protocol with a passphrase of at least 20 characters, is mandatory for wireless security. If WPS is available on the router, it should be turned off, then verify that it is truly disabled, as a number of devices currently on the market don’t disable it even when instructed to. Finally, don’t bother with ineffective WiFi security options, such as MAC address filtering or disabling SSID broadcast.

The last step in personal information security is not especially IT related. Personal information leakage through paper documents is far too easy. Paper documents containing personal or financial information should be shredded prior to disposal or recycling. Similarly, media devices such as CD/DVD ROM media, hard drives, or USB sticks should be physically destroyed or securely overwritten with special software before disposal. Last, one’s online presence can be a significant source of information leakage. Employees and children alike should be trained to not post personal details or details of company plans on Facebook or Twitter.

By internalizing these concepts, you can help build a culture of security. Thinking “secure first” may seem paranoid, but will enable your organization to navigate future threats and breaches. Does this make you invulnerable to a major breach or catastrophe? No! Certainly not, but it does enable quick response to minimize the damage from the event. Furthermore, it might just make you and your organization a slightly less desirable target to external malicious attacks or internal incidents.

The only promise that we can make is that security will continue to be at the forefront of IT challenges for many years if not decades to come. Additionally, the security solution that you put into place yesterday may not be applicable in a month, week, or even today! But a well thought-out security plan can adapt to changing technological measures, and carry your organization into the future.
References


Author Biographies

Glen Sagers is an Associate Professor at Illinois State University, teaching networking and security courses. His research interests include information assurance and security topics and open source software. He has published articles about the processes used to create open source software, and wireless security. A special ongoing interest is in practical security for home users and others uneducated in IT security. He received his Ph.D. from Florida State University.

Bryan Hosack currently works as a Senior Analyst in Business Intelligence, Reporting and Analytics in the financial industry. He has worked and consulted in a variety of IT areas across a variety of industries in addition to teaching a variety of IS and Computing subjects at Illinois State University. Bryan has published across a broad range of IT topics, including data and analytics, IT education and training, as well as wireless networking and security. Bryan has actively participated in MWAIS since 2011 and served as the conference Chair for the 8th Annual MWAIS conference. He received his Ph.D. from Florida State University.