

COMPUTER SECURITY & PRIVACY

Wednesday, October 19, 2011

By comsec on GET

Contents

Online Privacy – What we need to consider	3
Who are Hackers and what do they Do?	5
The 12 Scams of Christmas	6
Charity Phishing Scams	6
Email Banking Scams.....	6
Holiday e-cards.....	6
Fake Invoices	7
You've Got a New Friend!	7
Dangerous Holiday-related Search Terms	7
Coffee Shop Cybercriminal.....	8
Password Stealers	8
Fraud via Auction Sites.....	9
Holiday-themed Email Attachments and Spam	9
Online Identity Theft	9
Laptop Theft.....	10
Top 12 Ways to Protect your Online Privacy	11
Do not reveal personal information inadvertently.....	11
Turn on cookie notices in your Web browser, and/or use cookie management software or infomediaries.....	11
Keep a "clean" e-mail address.	13
Don't reveal personal details to strangers or just-met "friends".....	14
Realize you may be monitored at work, avoid sending highly personal e-mail to mailing lists, and keep sensitive files on your home computer.	14
Beware sites that offer some sort of reward or prize in exchange for your contact information or other personal details.....	15
Do not reply to spammers, for any reason.	15
Be conscious of Web security.	16
Be conscious of home computer security.....	17
Examine privacy policies and seals.	18
Remember that YOU decide what information about yourself to reveal, when, why, and to whom.	18
Use encryption!.....	19
Summary	20

Online Privacy – What we need to consider

You can have Security without Privacy, but you cannot have Privacy without Security. This is important to us as we move towards a new way of life.

An analogy useful in defining the way in which Security can afford you Privacy is the concept of a house being built. A house of course has to have a foundation. Walls are constructed; the plumbing and wiring are built into the walls, door frames, window frames and stairs are put in. Eventually the house is finished. When you approach a bedroom, you notice that there is a door, with a knob. This might make you stop, and knock on the door. We do this because we respect the Privacy of the person whose bedroom it is. The door itself, and to a more granular level the lock that may be in place in the door knob are considered **Physical Security Controls**, and they are considered **preventative controls**.

When you gain access to the bedroom, you notice that there are windows in the bedroom. During the day you want to be able to see out the window, and perhaps even have the window open. While we want to be able to see out, we don't necessarily want people to see in. During the day, unless the ambient light in the bedroom is stronger than the sunlight outside, you won't be able to see through the window from the outside. When the sun starts to set, however, you will probably want to lower the window shade. So far we have described a

- Standard: Protect the house occupant's privacy
- Policy: At sunset, lowers the blinds so that people can't see in

We know what our home policy states, but how do we accomplish that. If we have children in the house, we need to teach them the:

- Procedure:
 - Grasp the strings hanging down from the right hand side of the window-blind
 - Slightly pull the strings down together
 - Move a little bit to the right
 - Slowly release the tension you have on the strings, and allow gravity to let the window blind lower to the bottom of the window.
 - Control the speed of the blind being lowered, by continuing to keep tension on the strings, so that the blind doesn't crash to the bottom of the window, perhaps damaging the blind.

Once the older kids learn this Privacy Standard, the Policy that allows the standard to be enforced, and the Procedure to enable the Policy to be assured, the Culture of Compliance comes into play. Older kids will then be able to pass along what they have learned to the younger kids and lessons are learned about Privacy, and how to enable that privacy.

I use this simple example to show that without the security controls, we cannot have privacy. While everyone reading this document probably already knew how to lower blinds in a bedroom, it is most likely a practice that is done without much thought. This is because at one time you learned this, and it has become so ingrained in your daily life that is simply something that you do, without thought.

Hopefully the things you will learn to protect your Identity, your assets, and your and your family's safety will become just as routine.

The following pages are a synopsis of methods that hackers and wannabe hackers routinely use to steal and cause strife. This paper is not intended to cause fear. It is intended to list the vulnerabilities, or exposures that may be in place in

your own **information system**, and how you can close those exposures and lessen the risk of hacker's activities. In this paper, we will define your information system as best people, practices, systems, and processes.

One of the first things we need to do, to start planning to protect our information system, is to take inventory of who and what makes up that system. My own system consists of:

1. Computers
2. Computers that are temporarily on my network (guests, kids here for the weekend, etc.)
3. Printers
4. Switches
5. Copiers
6. routers (both hardwired, and wireless)
7. switches
8. scanners
9. external hard drives
10. thumb drives
11. cd/dvd rom drives
12. smart phones
13. people I share information with (family, colleagues, and clients)
14. methods in which I share that information (verbally, electronically, on paper)

Lots of people will have one computer, and a printer. Others will have home networks. Regardless of the size and complexity of our information system, we need to exercise the same due diligence in protecting our information, assets, and the people in our lives.

Once we have an inventory of what constitutes our Information System, we need to know where our confidential information lives within our system, and what **data flows** we employ in using that information.

Since we are coming up on a Holiday Season, I thought it would be good to share research that describes the top 12 Scams of Christmas, provided by McAfee, and the Top 12 Ways to protect Your Online Privacy, by the Electronic Freedom Foundation. A Glossary of common Security & Privacy words and Phrases is at the end of the document.

Who are Hackers and what do they Do?

Hackers come in many different shapes and sizes. From script kiddies to State-Sponsored (read some government) groups (picture hundreds of people sitting at a table in a warehouse, each with a computer in front of them), and a high-bandwidth internet connection, many different types of hackers exist. While hacking used to be an individual thing, there are now many groups of disparate people working together to the same end. Today, one of the largest reasons is to steal identities, and financial information. There are thousands of examples to use.

One recent and successful hacker activity leveraged the credit card point of sale system that 2 resorts vending machines were connected to. I am talking coke machines, and vending machines that you buy crackers from. They weren't interested in stealing the money, but in the past two years they were able to steal 40,000 people credit card information, right down to the pin numbers. There is a huge market in printing new credit cards, using the embedded information from stolen information to code these new cards.

Another individual (one person's hacking endeavors) is illustrated when in July of this year he was found with 675,000 stolen credit card numbers. Use of these numbers resulted in the loss of \$36 million dollars; actually a small amount, considering all of the numbers he had. Remember, the theft of credit card information may not be apparent, as they don't want you to know they have gotten your information.

Once last example is that there are "internet back-alley" websites that are well known in the hacker community, and becoming better known to the people combatting cybercrime where someone can go to "buy" active bank account and credit-card information. For prices that are on a scale, someone can buy an account that is 'guaranteed' to have \$8,000 in it, for 10-15 days. The back-alley websites change virtual locations rapidly, and is done through proxy servers that may show that the site is located in Europe, when in fact the perpetrators are somewhere in Africa. Very hard to catch.

These are just a couple of examples of how people steal identities, and assets. Left undetected, it can and has been catastrophic for many. Clearing your name might be done in time; recovering your assets is questionable. Regardless, this is strife that can be avoided, if we are proactive in protecting ourselves, our assets, and our personal information systems. The following pages include information from McAfee, and The Electronic Frontier Foundation.

Links to specific products and other information is subjective, though I personally have been working deeply with McAfee for many years, with their Enterprise Core Products for Encryption, and Data Loss Prevention. I have worked side by side with many program managers, product managers, trainers, programmers and support resources. I have architected, implemented, and trained solutions and products for organizations from Ivy League Universities to globally dispersed Fortune 500 companies, to Health Systems with hospitals across many states. I personally support McAfee's products.

The 12 Scams of Christmas

http://home.mcafee.com/advicecenter/Default.aspx?id=ad_cybercrime_1soc

Bad Santas are making their lists and checking them twice, gearing up to rip off consumers online with common scams that take the happy out of the holidays.

Below, McAfee reveals their dirty tricks to educate the millions of consumers worldwide who want to enjoy safe shopping this holiday season.

Charity Phishing Scams

Many popular charitable organizations encourage consumers to think of others during the holiday season through emails asking for year-end donations. In fact, according to McAfee's recent holiday survey, almost 30% of US consumers plan to donate online this year.

Unfortunately, hackers also know consumers are in the giving spirit during the holidays and prey on their generosity through fake charity phishing emails.

Here's how it works: The hackers send fictional emails that appear to be from well known charitable organizations, such as the Red Cross, the Salvation Army, and Oxfam that direct consumers to fake websites designed to steal their money. The websites are generally very professional with a fairly high amount of graphical content and a good amount of verbiage designed to make the reader feel upset or guilty. Sometimes the layout and content of these fraudulent sites are copied directly from legitimate charity websites with simply a name and a logo changed.

To determine if an organization's site is legitimate, go directly to their Website to donate. Don't ever click on a link sent in email. To learn more about phishing, visit www.mcafee.com/advice.

Email Banking Scams

The current economic climate is not only forcing over 95% of us to spend less money and buy fewer holiday gifts this season, but prompting hackers to take advantage of our bank account balance concerns to bah-humbug the holidays with another common phishing scam.

Financial institutions are the most common phishing scam targets. According to the Anti-Phishing Working Group, during the first quarter of 2008, 92% to 94% of all phish scams were financial-services related.

With these scams, the bad guys send an official-looking email that asks consumers to confirm account information, including their user name and password. These emails often try to fool consumers into thinking that if they don't comply with the instructions, their account will become invalid.

So remember, call your bank by telephone if you're concerned about your account. Never give your account details out as a result of an email request or you could fall victim to a popular phish scam designed to empty your wallet. And with the stress of the holidays, your guard might just be down enough that you fall for one of these scams.

Holiday e-cards

Most people never consider the dangers of e-cards -- but unfortunately, there are plenty of dangers, especially during the holiday season. For example, a scam that was popular in 2007, was a New Year's e-card that included a nasty surprise. When the consumer clicked on the link, they were brought to a malicious Website that

attempted to download Trojan software.

Here's another tricky example: Scammers may send you an e-card that appears as if it's coming from Hallmark asking you to download an attachment to pick up your e-card. However, the attachment isn't really an e-card -- it's a Trojan. This particular Trojan then waits for you to sign onto AOL. If and when you do, it displays a pop-up window that looks like an AOL form, but asks you to verify/update your AOL billing info by providing your credit card, checking account info, and Social Security number.

A few clues that an e-card is not legit are spelling mistakes, errors in the message, unknown senders or senders with bogus names and odd-looking URLs.

Remember – if in any doubt about the legitimacy of an e-card, don't open it. Never click on anything from an unknown source.

Fake Invoices

During the holidays, lots of friends and families order and send gifts online. This is no secret to stealthy Scrooges who try to trick consumers into giving away personal financial details through fraud invoices.

Here's how this scam works: The bad guys create a fake invoice or waybill and send it via email as an attachment. Once the consumer opens the email attachment there are a few variations of - the recipient may be asked to confirm or cancel an order, they may be told that the parcel service was unable to deliver a package due to having an incorrect address, or the recipient may receive a customs notification about an international package.

In every instance, the email either asks the consumer for their credit card details so that their account can be credited or requires the recipient to open an invoice or customs form to receive the package.

Pretty tricky, huh? This kind of scam has been played on many consumers who believed they were receiving emails from FedEx, UPS or the US Customs Service but instead were delivered a deadly Trojan program or other threat that can lead to identity theft or hacker control of a computer.

To protect yourself, never give your financial details over email to an unknown recipient or open a suspicious attachment. If you want to ensure you are reaching shipping sites like FedEx or UPS, open a browser and directly access the Website. Also, ensure that your Internet security software is up to date to help spot Trojans and other forms of malware if you have opened a bad attachment.

You've Got a New Friend!

As the joy of the holiday season brings people together and reignites old friendships, many of us are excited when alerted with a message that says, "You've got a new friend!" when using popular social networking sites.

Sadly, in some cases, after clicking on the notice, you NOT only do not have a new friend—you have downloaded malicious software that you can't even detect. Of course, it's designed to steal personal and financial information. Stay away from "friends" you don't know.

Dangerous Holiday-related Search Terms

We love Santa too, but when clicking on the results of a "free Santa download" search, in addition to the Christmas-themed screensavers, puzzles, and pictures you find, you also could be clicking on adware, potentially unwanted downloads, and spyware.

In fact, McAfee's free and award-winning safe search tool, McAfee® SiteAdvisor®, found that all of the following holiday-related search terms are risky:

- Free Santa holiday screensaver
- Free holiday screensaver
- Free Christmas screensaver
- Free holiday downloads
- Christmas tree download
- Free Christmas wallpaper
- Santa wallpaper
- Santa screensaver
- Santa ringtones
- Santa mail download
- Santa download
- Free Santa music downloads

When searching for fun holiday-themed downloads, make sure your holiday searches are guided by McAfee SiteAdvisor software—the simple green, yellow and red rating system will help you avoid any unwanted gifts you may get along with your Christmas downloads.

Coffee Shop Cybercriminal

While everyone enjoys a warm gingerbread latte while surfing the Net at their local coffee shop, most are not aware of the dangers in surfing on unsecured networks. Attackers can jump on an unsecured wireless Internet connection with a program called a packet sniffer to see what Websites users are visiting, the passwords they are using, and what bank accounts they are accessing.

Also, an attacker might set up a rogue wireless access point nearby a coffeehouse. If somebody unwittingly connects to the attacker's network, the miscreant can watch just about everything that goes on while that connection is in use and can redirect traffic, sending the unknowing user to the dark alleys of the Internet.

McAfee advises consumers to make sure they have updated security software including a firewall, they've updated the patches on their system—and most importantly, they check bank accounts and shop online from a known, secure wireless Internet connection.

Password Stealers

The McAfee holiday shopping survey found that 53% of consumers admit they use the same password for multiple websites or online services. Consumers need to know that free and low-cost tools exist that make it easy for bad guys to guess passwords and hack into users' PCs. That's a holiday visit no one wants.

McAfee Labs found that attackers go after passwords for banks and e-commerce sites, multi-player online role playing games, instant messaging and finally, social networking sites.

As tricky as getting malware that's delivered invisibly via spam, consumers could get a password stealer downloaded to their PC without even knowing it.

By using the same password, an attacker only has to nab one password to hit all of a user's accounts. So this holiday season, be sure you use have an updated comprehensive security software suite to help prevent access

to password-stealing malware. This includes anti-virus, anti-spyware and a two-way firewall. Remember to check to make sure your subscription software is current – and not just trial software that might be expired.

In addition, create complex passwords such as: \$aNt@IsRe@l or H@PPyH0!d@y\$. [Check out these tips on how to create safe passwords.](#)

Fraud via Auction Sites

As nearly 40% of American consumers are expected to visit auction sites to find gifts this holiday season, shoppers must be aware of scammers who will use the increased activity of the holiday season to prey upon new victims. Be sure to read the security and safety policies from such sites as [eBay](#). You'll learn how to protect your account and buy safely

eBay's Online Safety Advisor, Rich LaMagna, recommends the following:

- Use your common sense. If an item looks too good to be true, it probably is.
- Carefully review the seller's ratings and feedback to be sure that he or she has a positive rating. Learn more about the item before bidding on it by carefully reading all of the information in the item listing, including the seller's policies.
- Pay with a safe payment method such as PayPal or your credit card. These methods offer the most protection for buyers should something go wrong with the transaction. To learn more about eBay's Buyer Protection Program, click [here](#).

Holiday-themed Email Attachments and Spam

The bad guys know that emails with holiday-inspired subject lines are intriguing to most consumers. The recent McAfee holiday survey found that 49% of consumers have opened or would open an email with a holiday themed attachment.

Consumers should beware of emails that prey upon their holiday spirit, inviting them to look at homes bedecked with lights or PowerPoint presentations with vague holiday-related subjects. For example, last year an email made the rounds with a Microsoft PowerPoint called "Christmas Blessings" that contained malicious software.

Some examples of subject lines bad guys use to lure consumers into opening a friendly-looking email are "happy 2008 to you!", "happy 2008!" and "new hope and new beginning". Be wary when you see these titles and don't open attachments with odd-looking URLs.

Online Identity Theft

Online shopping offers the 3 Cs: cost, convenience and choice, but there's one more we learned about from the McAfee Shopping Survey: concern.

90% of consumers have some level of concern about shopping online. Unsure of where to shop, they rely on friends and family to determine the safety of a website, but friends can only advise on personal experiences, and some sites may have security issues that aren't readily apparent.

For example, sites that store your personal information can be vulnerable to cybercriminals who hack in to steal your identity. In fact, research shows that as many as 80% of websites have known vulnerabilities.

McAfee can help. The McAfee SECURE™ trust mark appears on more than 80,000 sites that pass daily testing for more than 10,000 known hacker vulnerabilities. Your personal information is safer on sites tested by McAfee

SECURE because daily scanning for known threats can prevent Websites from falling prey to the vast majority of hacker crime. Only valid sites that pass the McAfee SECURE service of daily testing can display the trustmark.

Laptop Theft

And the last way the bad guys can take the merry out of your Christmas is by outright stealing your laptop! According to the FBI's State of the Net Report (2007), chances of having a laptop stolen are 1 in 10, and according to the research firm Gartner, 97% of laptops are never recovered.

While you are out enjoying the festivities of the season, make sure to be particularly vigilant at this time of year and never leave your laptop in sight in your car.

For further protection, be sure to purchase a product that safeguards important files – including photos, music and bank/credit card statements, in the event your laptop is stolen. One such product is [McAfee Anti-Theft File Protection](#) software.

Top 12 Ways to Protect your Online Privacy

Electronic Frontier Foundation - <https://www.eff.org/wp/effs-top-12-ways-protect-your-online-privacy>

Do not reveal personal information inadvertently.

You may be "shedding" personal details, including e-mail addresses and other contact information, without even knowing it unless you properly configure your Web browser. In your browser's "Setup", "Options" or "Preferences" menus, you may wish to use a pseudonym instead of your real name, and not enter an e-mail address, nor provide other personally identifiable information that you don't wish to share. When visiting a site you trust you can choose to give them your info, in forms on their site; there is no need for your browser to potentially make this information available to all comers. Also be on the lookout for system-wide "Internet defaults" programs on your computer (some examples include Window's Internet Control Panel, and MacOS's Configuration Manager, and the third-party Mac utility named Internet Config). While they are useful for various things, like keeping multiple Web browsers and other Internet tools consistent in how they treat downloaded files and such, they should probably also be anonymized just like your browser itself, if they contain any fields for personal information. Households with children may have an additional "security problem" - have you set clear rules for your kids, so that they know not to reveal personal information unless you OK it on a site-by-site basis?

Turn on cookie notices in your Web browser, and/or use cookie management software or infomediaries.

"Cookies" are tidbits of information that Web sites store on your computer, temporarily or more-or-less permanently. In many cases cookies are useful and innocuous. They may be passwords and user IDs, so that you do not have to keep retyping them every time you load a new page at the site that issued the cookie. Other cookies however, can be used for "data mining" purposes, to track your motions through a Web site, the time you spend there, what links you click on and other details that the company wants to record, usually for marketing purposes. Most cookies can only be read by the party that created them. However, some companies that manage online banner advertising are, in essence, cookie sharing rings. They can track which pages you load, which ads you click on, etc., and share this information with all of their client Web sites (who may number in the hundreds, even thousands.) Some examples of these cookie sharing rings are DoubleClick, AdCast and LinkExchange. For a demonstration of how they work, see: <http://privacy.net/track/>

Browsers are starting to allow user control over cookies. Netscape, for example, allows you to see a notice when a site tries to write a cookie file to your hard drive, and gives you some information about it, allowing you to decide whether or not to accept it. (Be on the lookout for cookies the function of which is not apparent, which go to other sites than the one you are trying to load, or which

are not temporary). It also allows you to automatically block all cookies that are being sent to third parties (or to block all cookies, entirely, but this will make some sites inoperable). Internet Explorer has a cookie management interface in addition to Netscape-like features, allowing you to selectively enable or disable cookies on a site-by-site basis, even to allow cookies for a site generally, but delete a specific cookie you are suspicious about. With Internet Explorer you can also turn on cookies for a site temporarily then disable them when you no longer need them (e.g., at an online bookstore that requires cookies to process an order, but whom you don't want to track what books you are looking at, what links you are following, etc., the rest of the time.) Turning on cookie warnings will cause alert boxes to pop up, but after some practice you may learn to hit "Decline" so fast that you hardly notice them any more. The idea is to only enable cookies on sites that require them AND whom you trust.

You may also wish to try out "alternative" browsers like Mozilla (Windows, Mac, Linux), Opera (Windows, Mac, Linux), Konqueror (Linux), and iCab (Mac), which may offer better cookie management.

You can also use cookie management software and services. One example is the Internet Junkbuster Proxy (<http://www.junkbusters.com/ht/en/ijb.html>). It runs on Win95/98/NT and

Unix/Linux

(no Mac version), and can selectively block cookies for you (and banner ads, to boot). interMute (<http://www.intermute.com/>)

does likewise (and more - blocks popup windows, etc.; only runs under Windows).

Another Windows-only solution is AdSubtract (<http://www.adsubtract.com/>)

A comparable product (Linux, Solaris, Windows) is GuideScope (<http://www.guidescope.com/home/>)

A Java-based solution called Muffin (<http://muffin.doit.org/>) is also available. While it will run on Mac, Windows and Unix systems, it is definitely for "power users", as it is complicated to set up and operate effectively.

Another recent option (Linux, Mac, Windows) is the

(<http://www.webwasher.com/>), which has advanced cookie filtering capabilities, especially with the Seclude-It and Secretmaker plug-ins available at the same site. One more (Windows) is CookiePal (<http://www.kburra.com/cpal.html>), and yet another (Windows) is (<http://www.thelimitsoft.com/cookie.html>).

There are also numerous "cookie eater" applications, some which run on a schedule or in the background, that delete cookie files for you. As with turning off cookies entirely, you may have trouble accessing sites that require certain cookies (though in most cases the worst that will happen is that you'll have to re-enter a login ID and password

you thought were saved.) "Eating" the cookies periodically still permits sites to track what you're doing for a short time (i.e., the time between successive deletion of your cookie file), but thwarts attempts to discern and record your actions over time.

Yet another option is to use an "infomediary" (some are home-use software products, others may be network-based services),

such as SeigeSoft's

SiegeSurfer (<http://www.siegesoft.com/html/tutorial.asp>),

Zero Knowledge Systems' Freedom

(<http://www.freedom.net>), among others. These products/services act as a proxy or shield between you and sites you visit, and can completely disguise to Web sites where you are coming from and who you are (and intercept all cookies). Most are Windows-only at this point, though Orangatango (<http://www.orangatango.com/>), and SafeWeb

and (<http://www.safeweb.com>) also offer such services that are Web-based and not platform-dependent.

WARNING: Do not confuse honest infomediaries with "identity managment services" like Microsoft's Passport service or Novell's DigitalMe. While you may gain some temporary convenience at sites that support them, you'll lose essential privacy, because these services are not there to serve you but to serve marketing purposes by collecting a vast array of information about you and selling it.

The best solution doesn't exist yet: Full cookie management abilities built into the browsers themselves. Only increased user pressure on Microsoft, Netscape and other browser makers can make this happen. Users should ultimately be able to reject cookies on a whole-domain basis, reject all third-party cookies by default, reject all cookies that are not essential for the transaction at hand, receive notice of exactly what a cookie is intended for, and be able to set default behaviors and permissions rather than have to interact with cookies on a page-by-page basis. This just isn't possible yet. You may wish to contact the company that makes your browser software and demand these essential features in the next version.

Keep a "clean" e-mail address.

When mailing to unknown parties; posting to newsgroups, mailing lists, chat rooms and other public spaces on the Net; or publishing a Web page that mentions your e-mail address, it is best to do this from a "side" account, some pseudonymous or simply alternate address, and to use your main or preferred address only on small, members-only lists and with known, trusted individuals. Addresses that are posted (even as part of message headers) in public spaces can be easily discovered by spammers (online junk mailers) and added to their list of targets. If your public "throw away" address gets spammed enough to become annoying, you can simply kill it off, and start a new one. Your friends, boss, etc., will still know your "real" address. You can use a free (advertising-supported) e-mail service provider like Yahoo Mail or Hotmail for such "side" accounts. It is best to use a "real"

Internet service provider for your main account, and to examine their privacy policies and terms of service, as some "freemail" services may have poor privacy track records. You may find it works best to use an e-mail package that allows multiple user IDs and addresses (a.k.a. "personalities", "aliases") so that you do not have to switch between multiple programs to manage and use more than one e-mail address

(though you may have to use a Web browser rather than an e-mail program to read your mail in your "throw away" accounts - many freemail providers do not allow POP or IMAP connections). If you are "required" to give an e-mail address to use a site (but will not be required to check your mail for some kind of access code they send you), you can use "someuser@example.com" (example.com is a non-existent site, set up by the Internet standards to be used as an example that will never accidentally coincide with anyone's real e-mail address, which is always a danger if you just make up one off the top of your head.)

Don't reveal personal details to strangers or just-met "friends".

The speed of Internet communication is often mirrored in rapid online acquaintanceships and friendships. But it is important to realize that you don't really know who these people are or what they are like in real life. A thousand miles away, you don't have friends-of-friends or other references about this person. Be also wary of face-to-face meetings. If you and your new e-friend wish to meet in person, do it in a public place. Bringing a friend along can also be a good idea. One needn't be paranoid, but one should not be an easy mark, either. Some personal information you might wish to withhold until you know someone much better would include your full name, place of employment, phone number, and street address (among more obvious things like credit card numbers, etc.) Needless to say, such information should not be put on personal home pages. (If you have a work home page, it may well have work contact information on it, but you needn't reveal this page to everyone you meet in a chat room.) For this and other reasons, many people maintain two personal home pages, a work-related one, and an "off duty" version. In the commercial sector, too, beware "fast-met friends". A common "social engineering" form of industrial espionage is to befriend someone online just long enough to get them to reveal insider information.

Realize you may be monitored at work, avoid sending highly personal e-mail to mailing lists, and keep sensitive files on your home computer.

In most US states and many if not most countries, employees have little if any privacy protection from monitoring by employers. When discussing sensitive matters in e-mail or other online media, be certain

with whom you are communicating. If you replied to a mailing list post, check the headers - is your reply going to the person you think it is, or to the whole list? Also be aware that an increasing number of employers are monitoring and recording employee Web usage, as well as e-mail. This could compromise home banking passwords and other sensitive information. Keep private data and private Net usage *private*, at home.

See this *CNN/IDG* article on "snoopware" (which may not be limited to your office...):

<http://www.cnn.com/2001/TECH/ptech/11/07/snoopware.idg/>

Beware sites that offer some sort of reward or prize in exchange for your contact information or other personal details

There's a very high probability that they are gathering this information for direct marketing purposes. In many cases your name and address are worth much more to them because they can sell it to other marketers (who can do the same in turn...) than what you are (supposedly) getting from them. Be especially wary of sweepstakes and contests. You probably won't win, but the marketer sure will if you give them your information.

Do not reply to spammers, for any reason.

"Spam", or unsolicited bulk e-mail, is something you are probably already familiar with (and tired of). If you get a spammed advertisement, certainly don't take the sender up on whatever offer they are making, but also don't bother replying with "REMOVE" in the subject line, or whatever (probably bogus) unsubscribe instructions you've been given). This simply confirms that your address is being read by a real person, and you'll find yourself on dozens more spammers' lists in no time. If you open the message, watch your outgoing mail queue to make sure that a "return receipt" message was not generated to be sent back to the spammer automatically. (It is best to queue your mail and send manually, rather than send immediately, so that you can see what's about to go out before it's actually sent. You should also turn off your mailer's automatic honoring of return receipt requests, if any.) If you have a good Internet service provider, you may be able to forward copies of spam e-mail to the system administrators who can route a complaint to the ISP of the spammer (or if you know a lot about mail headers and DNS tools, you can probably contact these ISPs yourself to complain about the spammer.) If you are getting spammed a lot, there are a variety of filters and anti-spam services available, including:

Spam Hater (http://www.cix.co.uk/~net-services/spam/spam_hater.htm) for Windows users;

TAG (<http://alcor.concordia.ca/topics/email/auto/procmail/spam>) for experienced Unix users;

SpamBouncer (<http://www.spambouncer.org>) for experienced Unix users (works well with TAG);

BrightMail (<http://www.brightmail.com/>) for ISPs;

SpamCop (<http://spamcop.net/>) for anyone;

More information on fighting spam is available at:

Elsop's Anti-Spam Page (<http://www.elsop.com/wrc/nospam.htm>);

MaximumDownforce's Info-n-Links Page(<http://www.maximumdownforce.com/hotlinks.html>);

Whew's Anti-Spam Campaign (<http://www.whew.com/Spammers/>).

Many of these are difficult to use for novices, and some require Unix expertise. Others are services that deal with ISPs only, not end users.

Be conscious of Web security.

Never submit a credit card number or other highly sensitive personal information without first making sure your connection is secure (encrypted). In Netscape, look for an closed lock (Windows) or unbroken key (Mac) icon at the bottom of the browser window. In Internet Explorer, look for a closed lock icon at the bottom (Windows) or near the top (Mac) of the browser window.

In any browser, look at the URL (Web address) line - a secure connection will begin "https://" instead of "http://". If you are at page that asks for such information but shows "http://" try adding the "s" yourself and hitting enter to reload the page (for Netscape or IE; in another browser, use whatever method is required by your browser to reload the page at the new URL). If you get an error message that the page or site does not exist, this probably means that the company is so clueless - and careless with your information and your money - that they don't even have Web security. Take your business elsewhere.

Your browser itself gives away information about you, if your IP address can be tied to your identity (this is most commonly true of DSL and broadband users, rather than modem users, who are a dwindling minority). For a demo of how much detail is automatically given out about your system by your browser, see: <http://privacy.net/analyze/> .

Also be on the lookout for "spyware" - software that may be included with applications you install (games, utilities, whatever), the purpose of which is to silently spy on your online habits and other details and report it back to the company whose product you are using. One MS Windows solution for disabling spyware is the Ad-aware program

(shareware, from <http://www.javasoft.de/>), which can remove spyware from your computer; it is based on a large collaboratively maintained database of information about spyware. Linux and Mac products of this sort are likely to appear soon.

Java, Javascript and ActiveX can also be used for spyware purposes. Support for these scripting languages can be disabled in your browser's configuration options (a.k.a. preferences, settings, or properties). It is safest to surf with them turned off, and only turn them on when a site you trust and want to use requires them. If you don't know if your browser supports these languages or don't know if they are turned on you can use BrowserSpy to find out (along with a lot of other information about your Web browsing software): <http://gemal.dk/browserspy/>

Another form of spyware consists of "webbugs", which typically manifest themselves as invisible or nearly invisible image files tied to cookies and javascripts that track your Web usage.

See <http://www.google.com/search?hl=en&q=webbugs+%22web+bugs%22>

for more information on webbugs. See also this webbug FAQ, http://www.nthelp.com/OEtest/web_bug_faq.htm for more details.

Dealing with webbugs when they are embedded in an otherwise legitimate page is thorny, as there isn't a surefire way to distinguish between webbugs and run-of-the-mill image files. But see the Privacy Foundation's Bugnosis webbug detector (<http://www.bugnosis.org/> - Windows MSIE only). When webbugs are loaded into popup pages, the solution is to close the popups (usually a small page with an ad, though some of them are "micropages" that you can barely see. A few may even use javascript tricks to keep you from closing them. If this happens, close all other browser windows, then you should be able to close the bug window). Another tip for defeating webbugs is to reject any cookies from Doubleclick, AdCast, LinkExchange and other "ad exchange networks" (cookie sharing rings), and any other cookies that are not from the site you are currently visiting (most third-party cookies are basically webbugs). Lastly on this topic, be aware that HTML-capable e-mail programs and Usenet newsreaders make webbugs work in your e-mail and newsgroups. If your mailer or newsreader has an option to turn off cookie support, you should certainly do so. There is hardly any imaginable legitimate use for a cookie in an email or a newsgroup posting.

Be conscious of home computer security.

On the other side of the coin, your own computer may be a trouble spot for Internet security.

If you have a DSL line, broadband cable modem or other connection to the Internet that is up and running 24 hours (including T1 at the office without a firewall or NAT),

unlike a modem-and-phone-line connection, be sure to turn your computer off when you are not using it. Most home PCs have pitifully poor security compared to the Unix workstations that power most commercial Web sites. System crackers search for vulnerable, unattended DSL-connected home computers, and can invade them with surprising ease, rifling through files looking for credit card numbers or other sensitive data, or even "taking over" the computer and quietly using it for their own purposes, such as launching attacks on other computers elsewhere - attacks you could initially be blamed for. Firewall hardware and software is another option that can protect you from these kinds of attacks (available at any computer store; freeware and shareware implementations may be available at sites like <http://www.shareware.com> or <http://www.download.com>).

Examine privacy policies and seals.

When you are considering whether or not to do business with a Web site, there are other factors than a secure connection you have to consider that are equally important to Web security. Does the site provide offline contact information, including a postal address? Does the site have a prominently-posted privacy policy? If so, what does it say? (Just because they call it a "privacy policy" doesn't mean it will protect you - read it for yourself. Many are little more than disclaimers saying that you have no privacy! So read them carefully.) If the policy sounds OK to you, do you have a reason to believe it? Have you ever heard of this company? What is their reputation? And are they backing up their privacy statement with a seal program such as TRUSTe (<http://www.truste.org/>) or BBBonline (<http://www.bbbonline.org/>)? (While imperfect, such programs hold Web sites to at least some minimal baseline standards, and may revoke, with much fanfare, the approval-seal licenses of bad-acting companies that do not keep their word.) If you see a seal, is it real? Check with the seal-issuing site to make sure the seal isn't a fake. And examine terms carefully, especially if you are subscribing to a service rather than buying a product. Look out for auto-rebilling scams and hidden fees.

Remember that YOU decide what information about yourself to reveal, when, why, and to whom.

Don't give out personally-identifiable information too easily. Just as you might think twice about giving some clerk at the mall your home address and phone number, keep in mind that simply because a site asks for or demands personal information from you does not mean you have to give it. You do have to give accurate billing information if you are buying something, of course, but if you are registering with a free site that is a little too nosy for you, there is no law (in most places) against providing them with pseudonymous information. (However, it would probably be polite to use obviously fake addresses, such as "123 No

Such Street, Nowhere, DC 01010". If they are generating mailings based on this information - presumably in accordance with the terms of their privacy policy - they can probably weed such addresses out and not waste the postage on them. Definitely do NOT use someone else's real address!)

However, if you are required to agree to terms of service before using the free service, be sure those terms do not include a requirement that you provide correct information, unless the penalty is simply not being allowed to use the service any more, and you're willing to pay that price if they figure out you are not providing them with your actual personally-identifiable information.

Use encryption!

Last but certainly not least, there are other privacy threats besides abusive marketers, nosy bosses, spammers and scammers. Some of the threats include industrial espionage, government surveillance, identity theft, disgruntled former associates, and system crackers. Relatively easy-to-use e-mail and file encryption software is available for free, such as Pretty Good Privacy (PGP, available at: <http://www.pgpi.org/>), which runs on almost all computers and even integrates seamlessly with most major e-mail software. Good encryption uses very robust secret codes, that are difficult if not impossible to crack, to protect your data. You can also use specialized services (some free, some pay) that go beyond infomediary services, including running all connections through a securely encrypted "tunnel", anonymous dialup, even anonymous Web publishing. Another type of product is SSH tunnelling (port forwarding) packages, such as FSecure SSH (<http://www.fsecure.com/products/ssh/>), and SecureCRT (<http://www.vandyke.com/products/securecr/>).

Summary

Intel recently purchased McAfee. On some of Intel's computer chipset, encryption architecture exists that allows encryption to happen in hardware. Within the next 1-3 years, more encryption, and other computer security will be included in all ISP services and operating systems, but for now you have to actively seek out good service providers and add-on products.

While unable to assess every person's information system, and since all of our systems will be as different as we each are, I will say that a good start to securing a typical home system should include the services available in McAfee All Access 2012–Individual version. Retail prices are around \$ 99 USD. A data-sheet is available at http://download.mcafee.com/products/manuals/en-us/MAA_DataSheet_2012.pdf and the main information sheet is available at <http://home.mcafee.com/store/all-access-security>.

While this product includes a mechanism to provide 'container-based' encryption, I recommend more robust encryption than this. Encryption that would be more appropriate for our kind of need is available from TRUECRYPT and is FREE open-source disk encryption software for Windows 7/Vista/XP, Mac OS X, and Linux. This solution provides a mechanism to create a hidden Operating System, and hidden partition thus allowing you to have a person you would use under duress (someone forcing you to enter your password to give access to your computer (plausible deniability). Another password would be used to provide access to your real operating system and files. TrueCrypt can be reviewed and downloaded at <http://www.truecrypt.org/>.

I hope this document helps you wrap your arms around the threats that are out there, and how you can proactively defend against those threats. One of the most valuable defenses is to be informed. I hope this paper helps.