Cyber Security
How Not to Be A Fish

Paul S. Wang, Sofpower.com

May 18, 2023

The information highway that is the Web and the Internet makes life so easy and enjoyable for everyone everywhere. The *cyberspace* where communication over computer networks takes place has become must-have infrastructure for any modern society. However, in cyberspace, just like in physical space, bad things can happen. Such things include delivering unwanted/unwelcome materials, eavesdropping, breaking and entering, information theft, datanapping, and other cyber crimes. Surely, we want to take full advantage of the the Web/Internet while guarding against possible downsides.

In this third article, we will focus our attention on cyber security.

Widely publicized recent security breaches range from information theft to influencing democratic elections to holding computers for ransom. No wonder why many individuals feel edgy about their own security and privacy online. You are not alone if you feel unsure or even helpless.

While cyber security is a vast area and involves many factors and players—Internet providers, computer software and hardware companies, search engines, social media, and government agencies—here we focus only on a basic understanding of safety measures for individual users.

We will explain things clearly and provide practical advice on how to improve safety, spot dangers and avoid falling victim to various baits and lures that come your way in cyberspace.

We begin by talking about security attacks. Next, we will explain security measures regularly applied on the Web and Internet. Then, you will learn exactly what to do.

Cyberattacks

Let's first take a look at some high-profile cyberattacks in recent years (Figure 1).

Figure 1: Cyberattacks

- **Minneapolis public school system data breach and leak (2023)**: The well-known Medusa hacking collective took credit for the data breach and proved their involvement by leaking a sample of employee and student data to the dark web. The early March attack tied up computer systems and communications throughout Minnesota' s largest school system for several days.
- **Colonial Pipeline Ransomware Attack (2021)**: In May 2021, the Colonial Pipeline, a major fuel pipeline operator in the United States, fell victim to a ransomware attack. The cybercriminal group known as DarkSide was responsible for the attack, leading to the shutdown of the pipeline for several days and causing disruptions in fuel supply across the East Coast.
- **SolarWinds Cyberattack (2020)**: One of the most significant cyber attacks in recent history, the SolarWinds attack targeted the software company SolarWinds, allowing hackers to infiltrate their systems and gain access to numerous organizations worldwide. It is believed to

have been carried out by a Russian hacking group, resulting in the compromise of sensitive data and networks.

- **WannaCry Ransomware Attack (2017)**: The WannaCry ransomware attack (Figure 2) affected hundreds of thousands of computers worldwide. It exploited a vulnerability in Microsoft Windows systems and spread rapidly, encrypting files and demanding ransom payments in Bitcoin. The attack targeted various organizations, including healthcare institutions and government agencies.

Figure 2: WannaCry Ransomware Attack

- **NotPetya Cyberattack (2017)**: The NotPetya cyberattack was a destructive malware campaign that affected numerous organizations globally. It initially targeted Ukrainian businesses but quickly spread to other countries. NotPetya was disguised as ransomware but was later revealed to be a wiper, destroying data irrecoverably. The attack caused significant financial losses for several companies.

- **Equifax Data Breach (2017)**: In one of the most significant data breaches in history, the credit reporting agency Equifax suffered a cyber attack that exposed personal information of approximately 147 million people. The breach occurred due to a vulnerability in the company's web application software, allowing hackers to access sensitive data, including social security numbers and credit card information.

- **Sony Pictures Entertainment Hack (2014)**: A high-profile cyber attack targeted Sony Pictures Entertainment, leading to the leak of

sensitive data, internal emails, and unreleased films (Figure 3). The attack was attributed to the hacker group known as Guardians of Peace and was believed to be motivated by geopolitical tensions. The incident resulted in significant financial losses and reputational damage to Sony.

Figure 3: Sony Attack by Guardians of Peace

- **Target point-of-sale systems attack (2013)**: You may still remember that one day after Thanksgiving 2013, the large retail chain Target suffered a security breach. According to a *New York Times* blog, "Cybercriminals appear to have focused on the point-of-sale systems in Target's retail stores, which collect information from customers' credit and debit cards, and potentially personal identification numbers, or PINs." The stolen information can be used to create counterfeit credit or debit cards.

Cybersecurity attacks can be from a single individual or a well-organized group, some, the so-called *advanced persistent threat* groups, could be connected to industry or even governments.

A June 13, 2017 *Bloomberg News* article titled *Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known* said "*the Russian hackers hit systems in a total of 39 states*".

Generally, a cybersecurity attack exploits one or more vulnerabilities in your system or network, including the Internet as well as phone networks. Here are some types of attacks that should concern us end users.

- Phishing—Collecting private or confidential information such as userids, passwords, Social Security numbers, driver's license numbers, account numbers, phone numbers, PINs, addresses, and birth dates by tricking users to supply them through phone calls, emails, or fake websites (Figure 4). For example, an email may ask the user to increase email storage space, verify an online order, confirm a refund or payment, change login information, fix an old unpaid invoice, or manage a package delivery by clicking a link in the email. The link leads to an official looking online form put up by the attacker. Or, a scam may inform you of a sudden wealth that you can receive by sending your bank account information and often a handling fee or tax!

Figure 4: A Phishing Attack

- Spoofing—Pretending to be someone, at some IP address, from a certain website, sent from some email address, or located at certain GPS locations. Spoofing is usually done by falsifying data used in communication protocols. For example, the email sender (the `From` header) can be spoofed easily.

- Malware—Malicious software of all kinds including computer viruses, ransomware, worms (spreading themselves through the network), trojan horses (hiding in seemingly legit applications), keyloggers, spyware, and rogue security programs.

- Eavesdropping—Spying by secretly monitoring network communications or leaking electronic emissions from equipment. The man-in-the-

middle attack carries this further by intercepting messages between two correspondents, and perhaps even altering the messages as they are passed along to the other end.

Cyber crimes are a serious and global concern. Governments, private sectors, and academic institutions have acted to produce countermeasures, including legislation, regulation, law enforcement, protection of communication infrastructures, and *Computer Emergency Readiness Teams* (CERTs) in the USA and other countries.

Lock and Key

Security in cyberspace is not so different from that in physical space. In any case, there is no escaping from the need to deal with our own security in cyberspace. It may be a bother but there's no alternative.

How do we keep things safe in physical space? Is it not lock and key? The same goes for cyberspace. There, we want to keep our email account, bank account, online purchase accounts (Amazon or eBay account for example), memberships (Facebook, Twitter, LinkedIn, or Netflix membership for example), and so on under lock and key as well. These are known as *protected resources* online.

To unlock and access a protected resource, the key is usually a *userid-password* pair. Only the correct userid and password can unlock the protected resource and give you access. This process is usually called *login* or *signing in*. The assumption is that only the owner has the key and no one else does. Hence, we must do our best to keep it that way.

In cyberspace, the process of verifying the identity of a user in order to grant access to protected (locked) resources is known as *authentication*. The most common way of authentication for users is by userid and password.

Taking Care of Passwords

In physical space we need to take care of our lock and key. In cyberspace we must also safekeep our userid and password.

- Avoid short passwords. Use 12 or more characters that include uppercase and lowercase letters, numbers, punctuation marks, and special symbols. Keep your password easy to remember but hard to guess.

Don't use family names, 1234, 0000, or whole words. For longer passwords, consider a secret phrase.

- Don't use the same password in different places. This way, if a password were compromised, the damage would be limited to one place. But, this means that you will have many passwords, one for each of your accounts online.

- Write down your userid, password, and other authentication information (such as answers to security questions) somewhere safe. Consider saving them in a file kept offline (on a USB drive for example). It is best to also encrypt the file.

- When setting up answers to security questions, avoid using real answers and invent your answers instead. For example, use a fake birthday, mother's maiden name, hobby, model of first car, and so on. Record these in your file too.

- Change your passwords from time to time just to be extra safe.

- Make sure you are not being observed or video recorded when you log in. This is especially important when you are in a public place. Consider login to important places only from the privacy of your home. To be extra secure, set aside a computer for the sole purpose of doing important business online. Don't use that computer for any other purpose.

- Do not leave your computer or cellphone unattended after login. Lock the screen if you must leave for a short while. Always log out immediately after finishing your business. Close your browser or shutdown your system afterwards.

- Use the browser auto-login feature, where your browser remembers your userids and passwords for different websites, only if you enable a *browser master password* to protect the saved login information from others who may gain access to your computer. Select your browser's advanced security option to set your master password.

Dear Me, My Password!

You are not alone in feeling frustrated when you cannot remember a certain password. It happens to all of us, including those who never thought it possible for them. It is tempting to cop out and use the same password at many different places, making it easier to remember. Of course, that is unsafe and ill advised. Saving your passwords in a secure file is a good solution.

It is always possible to reset your password. Usually, *forgot my password* is an option at login time. Clicking on that option starts a process where you need to answer questions to establish your identity and to demonstrate that you are the owner of an account. The answers you provide will be checked against data stored in your account (your address, email address, phone number, security question answers, and so on) for verification. When things check out, you will receive an email with instructions for setting up a new password.

Your email address, being a way to identify your account and to send information to you and you alone, is critical in this whole password reset process. Therefore, it is important for you to make sure that no one except you can receive your email. It is never a good idea to allow someone else to handle your email.

The point is, if someone could receive your email that person would potentially be able to reset the password to some other account of yours, such as, goodness forbid, your bank account.

The same goes for your cellphone. A text message to your cellphone can be an alternative to email for resetting your password. And no one needs to be reminded that losing your cellphone is bad.

Encrypting Your Sensitive Data

The most sensitive data are *Personally Identifiable Information* (PII) because those data can uniquely identify you as a person and often used to determine the identity of a person (Figure 5). To keep files with sensitive data, such as PII, on your computer safe, you should encrypt them. For example, you may store scanned copies of family driver licenses, passports, birth certificates, stock certificates, and so on in files. It is a good idea to encrypt such files. The file with login info should be encrypted. Or use a password manager, such as LastPass, to store your passwords.

When a file is encrypted, it becomes a pile of scrambled garbage data

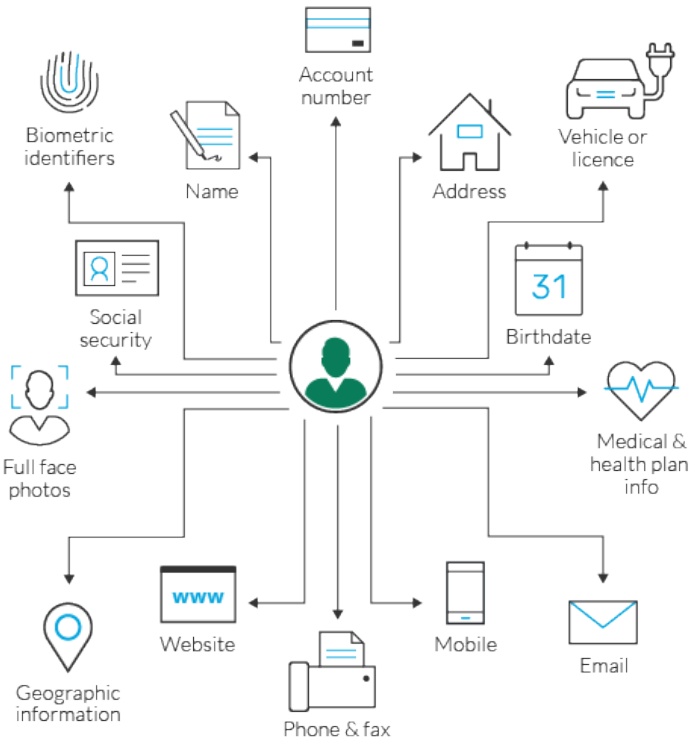

Figure 5: What IS PII

to anyone but the person who knows the key to decrypt the file back to its original readable form. Many tools are available for file encryption including Microsoft Word, LibreOffice, and AES Crypt, just to name a few. Be careful, forgetting the key for decrypting a file means the file will be lost forever. It is OK to use the same master key for all your encrypted files. Just make sure that key is secure and not used for any other purpose.

Back up your encrypted files. You don't want to lose these files if something happens to your computer.

Cybersecurity Habits

Organized countermeasures and the technologies on the Web and Internet for identification, authentication, encryption, and so on are all well and good. But, the human factor is still the weakest link in cybersecurity. As users in cyberspace, we all need to do our best to tighten security, and hopefully we

can collectively make cyberspace more secure for everyone.

Here are some suggested actions for individual users.

- Make sure system updates relating to security are installed as soon as possible.
- Enable firewalls and configure them correctly on your routers and computers. On your wireless router, use WPA2/WEP wireless security and turn off remote admin access.
- Download and install software only from known and trusted websites. Avoid FREE software that is too good to be true.
- Encrypt sensitive files on your computers and smartphones.
- Do not give your userid or password in response to an email or a phone call.
- **BACK UP** your important files on external disks (detachable from your computer), on flash drives, or on the cloud in encrypted form.
- Do not access your online accounts from public places or use borrowed computers.
- Keep your laptops, tablets, and smartphones with you all the time. Close down your Web browser after finishing with a login session. Lock the screen if you need to be absent for a short while. Do not leave them in your car or otherwise lying around!
- Be careful with flash drives and other similar free gift items. They may contain malware that can infect your computer.
- Be extra careful with Microsoft IE and Outlook; most security attacks target these applications due to their popularity. Consider using computers running Unix/Linux.
- For mobile devices, install apps only from official app stores, and enable the screen lock (and SIM card lock) features. Install an anti-virus app.

Do your best, and you'll be glad you did. If everyone does his/her part, cyberspace will be that much more secure.

Use Common Sense

When you receive an email with a fantastic deal that sounded too good to be true. It usually is. Do not open any attachments. Delete the email immediately.

To lore you in, phishing emails make up different stories such as online storage over quota, security policy changes, package delivery problems, and other clever tricks. Be suspicious, do not believe such stories without double checking on your own.

No legit business or organization will send email to a customer and give some excuse to ask for your userid and password. Neither will they give you a clickable link to enter such information. If you receive an email like that, it may indeed lead you to a phishing site where any information you enter will be stolen. You can spot the phishing site by paying attention to the browser `Location` box where the site URL is displayed. Is the URL the official company site? Is there a lock icon next to the URL? If not, get out of there immediately.

Web browsers will display a secure icon in the form of a *closed padlock* when HTTPS (secure HTTP) is in use. This means data traffic between you and the site is encrypted to prevent eavesdropping. Clicking on the lock icon reveals the *digital certificate* of the site. Examine the certificate to satisfy yourself that the site is not counterfeit.

To be safe, avoid clicking any link in an email or strange site. Always go to your intended site directly on your own by typing in its URL such as `bankofamerica.com`, `vanguard.com`, or `amazon.com`. Well-managed businesses and organizations usually send sensitive information to customers not by email but by messages placed in a secure inbox accessible only after login.

To avoid being swindled, we should never disclose personal information over email, by texting, by phone, or at a site not arrived on your own initiative. Let's all refuse to become a phishing victim.

It is good practice to never send any sensitive information over email unless it is encrypted. Overlook this and suffer the consequences. Imagine, we may have a different president in this country if the Democratic National Committee (DNC) staff had better sense of cyber security.

Reporting Cyber Attacks

Report email scams, phishing, Web forgery, and other security attacks you encounter immediately. Forward any suspected phishing email to

`3us-cert.gov/report-phishing`

or the Anti-Phishing Working Group `reportphishing@antiphishing.org`.

Contact authorities or the legitimate businesses to alert them. Use your Web browser's `Help->Report Web Forgery` option. Or contact the Internet Crime Complaint Center (`ic3.gov`).

You Can Do It

We have discussed the basics to protect yourself in cyberspace. All this may seem complicated and not particularly urgent for you. Nothing bad has happened to you or your computer. But when it happens it will be too late. Hopefully, by acting on some of the suggestions here, you'll start to make it safer. You don't have to do everything all at once. Make a start, and then I am sure you will become more confident to follow through.