STAYING SAFE ONLINE

Quick Guide

V 3.0

260135-1/1

Table of Contents

Introduction

Connecting to the Internet is most likely a natural part of both your work and personal lives today. In fact, it's so natural, you might not even give it a second thought. You connect to information, services, and entertainment daily via your computer, your smartphone or tablet, and your business laptop. A host of internet sites have your personal information--and that makes performing activities like shopping, social and professional networking, doing research, and sharing information easy and convenient. The beauty of online connectivity is that you can work, play, and access data online from almost anywhere, at any time.

This "always on" connectivity, however, comes with a price. Cyberattacks are on the rise. According to the Federal Communications Commission, criminals from almost 200 countries are online plotting attacks, some of them against governments and large corporations, and some of them against individuals like you. Cybercrime is recognized by the U.S. government and by security experts as the biggest threat facing Americans today. Your financial information, your private data, and your workplace are all at risk..

You might think you can simply lean on the experts--the IT professionals, security experts, and CIOs who make sure networks are secure and data is protected. But, the fact is, most data breaches occur not because the right protections weren't in place or because they failed. The majority of cybercrime--malware and virus infection, hacking and data breaches, denial of service attacks and compromised or lost data--are all the result of simple human error.

Fortunately, being aware of the risks, taking the right precautions, and being smart and safe when connected to the Internet can help you stay safe in the face of rising cybercrime attacks. Read on to learn what you can do to protect yourself.

Phishing and Other Types of Email Fraud

The CEO of a large corporation receives an urgent email from the Internal Revenue Service requesting information and alerting the company about a possible unclaimed tax refund. He is busy and gets hundreds of emails daily, but he figures since it's tax time this IRS request must be important, so he quickly forwards it to the CFO to take care of. The CFO receives the email, sees it is from the IRS and appears to be requesting information, and sends it on to the accounting and finance department with a note asking that it be taken care of immediately. The first thing the accounting specialist who retrieves the email from the department's email inbox notices are the names of the CFO and CEO in the email headers. He scrolls down to click on the IRS link and fills in the corporate tax ID number, account numbers, and other information the IRS is requesting on the simple form that pops up.

Unfortunately, the original email didn't come from the IRS, and it wasn't an innocent request. Instead, it was a fraudulent "phishing" email aimed at tricking corporate personnel into sharing private financial information about the company. When the accounting specialist filled out the information, it immediately fell into the hands of cybercriminals.

What Happened?

This corporation became the victim of "phishing," a type of cybercrime. A phishing victim receives an email on his or her computer or device that looks like it is from a legitimate organization, such as a bank, credit card company, government agency, or retailer. The email contains a link that takes the user to a malicious website or installs malware on the computer, which then infects the computer (and potentially the entire network if the machine is connected to one) with a virus.

In many cases, phishing scams play on people's emotions or fears to encourage them to click on the link or send personal information. For example, one type of

phishing scam involves an email stating "There is a convicted child predator living in your neighborhood," and contains a link and the name of a legitimate organization. The link actually takes the user to the organization's website, but in the meantime malware is being installed on the user's machine. Scams like this play on deep emotions and use phrases like "your local area" or "near your home" to lure you in. Don't let yourself get played by these criminals. Avoid clicking on anything that arrives in an email you didn't specifically sign up for or request via the organization or company itself.

How to Avoid Email Scams

Email is common vehicle for cybercriminals to use to spread malware, infect computers with viruses, and trick people into divulging private information so they can access financial accounts, corporate records, and other data. Be cautions when using email and follow these guidelines.

Beware attachments. Only open email attachments from a trusted source. Remember, most businesses, banks, retailers, government agencies, etc. won't send you information (such as an order confirmation or account update) as an attachment, but will send information in the body of an email.

Don't click links in email messages. Avoid clicking live links that are included in the body of an email. This is how most viruses and malware infect a computer. Hover over the link with your mouse to see the full URL of the site and check whether it is legitimate. Then, type the URL into your browser by hand.

Don't share personal information over email. Financial services such as PayPal, banks, retailers, government agencies such as the IRS, and other reputable companies won't ask you for information via email. Never provide information such as your Social Security number, a corporate tax ID, bank or credit card account numbers, social security numbers, or passwords over email.

Know the warning signs. Malicious emails often contain spelling errors, grammatical errors, or information that is slightly "off." For example, you might receive an email that uses your bank's colors and logo, but that contains strange capitalization errors and spells the company name wrong. It may also use urgent language compelling you to comply with a request to update your information or click a link to log in to your account. Reputable companies won't ask you to take these kinds of actions via email.

Beware email trails. Emails can get forwarded many times so it's difficult to tell who the original sender was. For example, the email may look like it came from your boss or a trusted friend, but the original email may have come from a fraudulent source. It is worth a few extra minutes to backtrack and figure out the original source.

Use a spam filter. Most email clients are equipped with a filter that will keep suspicious emails from reaching your inbox. You can also configure your email to filter out any suspicious or untrustworthy addresses or content. However, you still need to question every email that arrives in your inbox.

Steps to Take With Every Email You Receive

When You Receive an Email, Ask Yourself:

- Who is the original sender?
- Is it making an urgent request or playing on your fear and emotions?
- Does it appear to come from a legitimate source, but it's asking you for unusual information?
- Did you sign up to receive this email, or is it from an organization with which you are unfamiliar?
- Is it asking you to send personal information over the Internet? (remember, legitimate companies won't normally ask you to do this)

When in doubt, **don't open or click on anything**, and alert IT personnel.

When Files Are Held for Ransom

A small business owner arrived at his desk one morning to find a strange message on his computer screen: "Your files are locked. To get the key to decrypt them, you must pay $500 USD." The message also said that if the money wasn't paid within a week, the price would double. The business owner tried to access his files, but every one of them was locked up and inaccessible. He called a computer security expert, who informed him that he had become the victim of "ransomware." The malware could be removed from the computer, although this would be very expensive and time consuming. Plus, the files would still be lost forever if the ransom wasn't paid. The business was inoperable while the problem was ongoing, and the owner could not recover the files. Ultimately, he ended up paying the ransom using a form of Internet currency and buying a new computer.

How Does Ransomeware Work?

This business owner lost his files to ransomware called CryptoLocker. Ransomware is malware that infects a computer's hard drive and encrypts the files stored there. Users are locked out of their files unless they pay a ransom, usually in the form of internet currency or another untraceable method. The ransom usually increases if the user doesn't pay the ransom within a certain amount of time, and the files are permanently lost if the ransom remains unpaid. Files cannot be unlocked, even by security experts, once they are infected with ransomware, and the malware can spread to an entire network if the computer is connected to one, such as at a place of business.

In most cases, ransomware can be removed but the files cannot be recovered. Fines range from $50 or $60 to hundreds. According to security company Symantec, cybercriminals may earn in excess of $30,000 per day using this scheme.

Protect Against Ransomware and Other Malware

The absolute best step you can take to avoid the high costs associated with ransomware is to **back up your files regularly.** It's best to back up files to the cloud or to a hard drive or removable media such as a CD or flash drive that isn't connected to the network. That way, you will be able to recover important files in case of infection or malicious encryption. You can get rid of or clean the infected machine and remove the malware from your network, then recover your files from the backup.

Prevention steps:

- **Apply patches and software updates**. Set your computer and software programs to check for updates periodically or update automatically. This avoids having flaws in your system that could make your computer or network vulnerable to a cyberattack.
- **Install and update antivirus software.** There are many antivirus and antimalware programs available, ranging in cost from free to several hundred dollars, depending on your needs and budget. Make sure your computer is protected with at least basic antivirus software. Even more importantly, make sure the software is set to update automatically when you connect to the Internet and that it is set to scan your system regularly. Many users have antivirus software on their machines that hasn't been updated in months, or even years. Malware is constantly changing, and updated software will protect against the latest threats.
- **Use a firewall.** You can also purchase software that controls who and what can communicate with your computer over the internet. A firewall will block suspicious traffic that could indicate a cyberattack, and only let in communications known to be safe.
- **Configure your computer securely.** Your computer's web browser and other functionalities can be set so that it is harder to visit unsecure websites or take other potentially unsafe actions. This can be a help, particularly if you are inexperienced using a computer or share the machine with others who might be. Your computer vendor's help service should be able to assist you in configuring security settings if you don't know how to do it.

Even with all these security measures in place, you still need to be on alert . Cybercriminals are getting more sophisticated--and remember, their only aim is to get you to take some unintentional action that infects your computer or network. With that in mind, avoid clicking on pop-ups, ads, and email links. Ransomware is often downloaded to a computer when a user clicks on a seemingly innocent online ad or link. It then encrypts the files and demands the ransom.

File Sharing Opens the Door to Malicious Software

A loan officer at a multistate banking company was urged by her middle school-aged son to check out some new music he was listening to. Since she was rushing to get to work, he loaded it from his laptop onto a flash drive so she could bring it along. She arrived at work, poured herself a cup of coffee, logged in to her computer, plugged in the portable drive, and opened a music listening program. While she was listening to the new music, malware from her son's laptop infiltrated the bank's system, took over her computer, and began spreading. By lunchtime, the private financial information of thousands of customers had been compromised.

Unintentional Actions Can Have a High Cost

Many cyber "crimes" are unintentional, but they come at a high price. The loan officer's computer had to be scanned at length and repaired at great cost, and the entire network for the bank had to be taken offline for scanning and repairs. Customers had to be communicated with regarding the potential risk to their personal identities and financial information, and the bank had to pay for credit monitoring services for its customers for a year. In many cases, repairing a computer or network that has been infected with malware costs more than replacing it, and much important data is lost in the process. This event cost the bank thousands, and did untold damage to its reputation among customers.

Prevention Takes Caution and Common Sense

People often think that since the company they work for has state-of-the-art security and an expert IT department in place, it is immune from cybercrime and data breaches. However, the best system and the most knowledgeable personnel available can't take the place of common sense.

The fact is, the majority of breaches occur due to human error. Sometimes this "error" is intentional, as in the case where someone is trying to embezzle money from their employer. Most times, however, it's an accident that occurs in an eyeblink--the amount of time it takes to plug in a flash drive or click an email link.

Passwords Aren't Always Secure

Linda is a busy executive. She is always on the go, and it seems like she's always connected both to work and to her loved ones, whether by the smartphone in her hand, the laptop that's always in her bag, or the computers she has on her desks at the office and at home. She often works at home early in the morning or late at night. She also travels a lot for business, so she connects to the network at the home office while she's on the road so she can get work done over the hotel WiFi, at an airport hotspot, or even in the back of a cab.

Linda prides herself on being productive and always available to her clients, her colleagues, and her kids. But, after an incident last month she began rethinking whether all this "always on" connectivity was without risk. Linda accidentally left her smartphone on the table at a restaurant, and a thief was able to access all of Linda's passwords and accounts, and even get information off her company's network before she discovered the problem.

Linda learned that, even though she thought she was being careful, she still wasn't doing enough to protect her professional and personal information. Linda password protected everything, but she tended to use the same password over and over so she could remember it more easily. Plus, it was a password that could be guessed--the name of her dog and her oldest son's birthday.

Practice Password Hygiene

Chances are, you have dozens of passwords to access everything from your bank account to your email to your favorite shopping and social sites. Security experts agree that creating strong passwords is one of the best ways to protect yourself from cybercrime.

However, many people make egregious mistakes when it comes to passwords--using easily guessed words or series of numbers, reusing the same password over and over, or even using the word "password" as their password!

Cybercriminals use specially created programs to troll for passwords stored in databases for online retailers, financial institutions, and other sources. Once they find a password, they can plug it in to every possible site and location. If you use weak passwords or use the same password for everything, it's that much easier for cybercriminals to access your information.

Create Secure Passwords

Random combinations of upper and lowercase letters, numbers, and symbols are best. Avoid using recognizable words and phrases or series of numbers such as dates. One tip is to think of a sentence ("My dog likes to chase a yellow ball," for example), then use just the first letter of each word in the sentence. Convert one or two of those letters to numbers or symbols to create a stronger password.

More tips for creating passwords that are hard for cybercriminals to crack:

- **Don't reuse passwords.** Create an individual, strong password for every website, account, and device.
- **Use hardest passwords for most sensitive information.** Prioritize your passwords by using the strongest ones for your bank account, credit card websites, email, and other access points to your personal and financial information. Save simpler passwords for less sensitive sites.
- **Use two-factor authentication.** Some sites, such as banks and web-based email providers, offer you a two-step process to log in. The system will generate a random number after you sign in with your username and password, which is sent to a mobile device or a special token device. You enter that random number as well as your username and password to log in. That way, if your password is stolen from a password database, your information still cannot be accessed.
- **Change passwords regularly.** Change your passwords at least every 90 days, sooner if you suspect someone has accessed one of your accounts.
- **Keep passwords private.** Don't share passwords with anyone.

Secure Your Mobile Device

Even if you've taken precautions on your desktop or laptop, you may have a device in your pocket that is nearly as powerful and that has just as much (if not more) access to your personal information. Many people don't realize what a liability their mobile device can be when it comes to criminals being able to access information. Or, if you accidentally lose your phone like Linda did, it could become an easy way for thieves to access your information. For example:

- Many people use smartphones to access personal accounts, shop, and use social media. However, three in 10 smartphones aren't password protected and 41 percent aren't enabled for remote tracking and data wiping.

Only 22 percent of survey respondents said they read mobile app privacy statements before downloading apps.

Source: Edelman Berland survey for Experian's ProtectMyID, 2014 many Internet sites related to scholarship searches.

Protection Tips for Mobile Devices

Keep your mobile device from becoming a window into your private data if it is ever lost, stolen, or accessed by someone without authorization with these safety tips.

- **Lock your smartphone** with a strong password.
- **Understand your apps.** When you download an app, read the privacy policy so you understand what you are agreeing to. Apps may ask for permission to access your location data, social media profiles, or text messages, for example. Deny access to things you don't feel comfortable sharing.
- **Protect your number.** Only give out your mobile number to people you know and trust.
- **Watch out for fraudulent messages.** Just like when using email, avoid giving out personal information via text message or over the phone. Urgent requests to give out personal details such as account numbers or Social Security numbers via your mobile device are often scams.

- **Consider protecting your device** with security software that allows you to lock and wipe (delete) all the data from your phone remotely if it is ever lost or stolen.
- **Disable automatic connections.** Some phones connect to WiFi and/or Bluetooth automatically, which may enable them to connect to an unsecure network and transmit data without your knowledge.
- **Log out.** Especially if you shop, bank, access social media, or use other apps that access personal information on your phone, be sure to log out when you are done. It is all too easy for someone to pick up your mobile device and access your accounts if you remain logged on.
- **Avoid conducting financial or private business** on your phone, such as banking or accessing work data, when it is connected to a public WiFi hotspot.

Intentional Crime and Fraud

Businesses can be at risk for cybercrime that occurs purposefully, such as when a current or former employee accesses the network to steal or share information or embezzle funds. Businesses sometimes have systems that are insecure or processes that make it easy to steal or duplicate information. Consider the following:

In one temporary staffing services firm, the system that created and paid invoices was able to be accessed by nearly anyone in the company. A single person could create an invoice, and also pay it, rather than these functions being performed separately. This left the company at high risk for fraud.

It happened. A human resources administrator who oversaw the short-term and temporary employee payroll at the firm created fictitious temp employees and gave them her Social Security number and address. Over the course of several years, she paid these fictional "employees" $66,000.

In another case, a bank didn't perform systematic authentication for some types of transactions for high net-worth customers, instead counting on employees to recognize customers by voice on the phone. They did this in an effort to provide personal customer service.

The problem is, it backfired. Someone called in on a Friday before a long weekend requesting an urgent wire transfer. They sounded upset and their voice sounded unfamiliar, but the employee put it through because the bank was so focused on always providing the utmost in customer service. The money was wired into an account immediately. Unfortunately, the "customer" on the other end of the phone wasn't who they said they were, and the bank and its real customer became victims of fraud.

Be on the Lookout for Suspicious Activity

These types of crimes are not just security issues. They are also people issues. Unfortunately, there's only so far the best security in the world can take you if someone is intent on committing fraud or stealing data.

What to do:

- Be on the lookout for suspicious activity on the job, and report anything you feel is unusual.
- Don't let anyone bully or badger you into doing something that you know is outside of regulations.
- Trust your instincts and slow down. If something feels "off" to you, it is better to risk losing a single transaction, upsetting a client or supervisor, or missing a deadline than putting the entire company and/or individual private data at risk.
- If the network or your machine seems slow and sluggish, take note and say something to IT or your network administrator. In some cases, this indicates that malware or a virus is running or data is being accessed.
- Always log off from the network when you are not at your computer. Use a strong password to access the system, and don't share it with anyone.
- Don't access the network from unsecure personal mobile devices or bring in flash drives or other media from home or from a remote location.

IMPORTANT NOTE: Remember that if you haven't experienced a cybercrime, fraud, or security breach, you are more likely to have one occur than companies that have already been through it. Just because it hasn't happened yet doesn't mean you aren't at risk.

Learn best practices for keeping important data safe and secure, and follow them. ♦