Basic Security 1 – How to protect

Introduction

Welcome to the 21st century.

We live in an amazing time where we are instantly connected to the entire world.

We can communicate with anyone we want, anytime we want, anywhere we want.

In addition, we now have access to just about any information we need at our fingertips.

However, with all these amazing advances come new risks.

Now that the world is so easily interconnected it has become much simpler for cyber threats to attack and exploit our information.

As a result, we are committed to an active information security program.

In the following training we will discuss and learn who is targeting you, how you will be attacked and why.

In addition, we will teach you the steps you can take to protect yourself, your family and our organization.

You are the target

One of the most important things to understand is that you are the cyber criminal's primary target.

Many people have the misconception that cyber criminals target only large corporations or organizations, when in reality they also target individuals such as yourself.

In addition, while these attackers use a variety of sophisticated tools, the simplest way to hack into an organization is by targeting people.

Unaware employees are an organization's greatest weakness as people make common mistakes, such as clicking on malicious links or using an infected USB stick.

As a result you have become the primary target.

Your computer and your information has tremendous value to cyber attackers.

Some examples include:

Data Theft:
Cyber criminals can steal our highly confidential information by hacking your computer or compromising your work accounts.

Identity Theft:
Cyber criminals can steal and commit fraud with your personal information including your credit card data, medical history or bank accounts.

Attacking Others:
Cyber criminals can use your computer to harm others, including hacking other computers, launch denial of service attacks, or distribute spam.

This is why our organization has security policies and controls.

They are carefully designed to protect you and our organization, while also ensuring we are compliant with important standards and regulations.

This is also why it is so important that you understand and follow our security policies.

What you may not realize is you are also a target when you are traveling, such as at an airport, a hotel or attending a conference.

You are even under attack at home, when you and your family connect to the Internet.

To help protect yourself, your family and our organization, always remember some core principles:

Always be cautious and assume you are a target.

You may think you or your information does not have value but it does.

On the Internet attack are a constant.

If something seems suspicious or wrong, it most likely is.

Email and Messaging

Email is one of the most powerful attack methods in the cyber criminal's arsenal, simply because so many people depend on email in their daily lives.

What makes email so dangerous is cyber criminals can easily pretend to be someone or something you trust, such as your friend or your bank.

These email attacks, often called phishing, work by tricking you into doing something.

For example, here is an email sent by a cyber criminal pretending to be a well-known bank.

The email is very professional looking, including the bank's logo.

The email says there is a problem with your account and that if you do not update your account immediately, it will be deactivated.

It then requires you to click on a link and login to the website.

If you click on this link you are taken to a website that looks real, but in reality is a website controlled by the cyber-criminal designed to steal your information, including your login and password.

Keep in mind, many email attacks go beyond just stealing your information, their goal is to infect your computer.

For example, cyber criminals will send emails with links, just as we saw in the previous example.

However, instead of these links sending you to websites that steal your information, they take you to websites that silently hack your browser, infecting your computer and taking over it.

Or instead of links, criminals will send emails with infected attachments.

Here is an example of what appears to be an email from a legitimate organization, but in reality is an attempt by criminals to get you to open an infected attachment.

In addition to general phishing attacks, cyber criminals utilize a more targeted attack called spear phishing.

Spear phishing is a highly customized attack where only a few emails are sent to specific individuals within our organization.

These emails appear very realistic, often with a subject that is relevant to the victim's job or appear to come from individuals that the victim highly trusts.

Spear phishing attacks are harder to detect, but also require more work and research by the cybercriminal.

Another common email attack is scams.

These are messages telling you that there are millions of dollars sitting in Africa waiting for you to recover, or that you won the lottery, even though you never entered it.

The goal of these scams is to either get your money or your information.

The stories are often quite convincing, but are nothing more than cyber criminals attempting to fool you.

Finally, there is messaging.

Basic Security 1 – How to protect

Just like email, messaging can be used for many of the attacks we have discussed so far, such as on Facebook, Skype or on your smartphone.

Always be careful of messages, regardless of what technology you use.

In most cases simply opening an email or reading a message is safe.

For most attacks to work, you have to do something after reading the message, such as opening the attachment, clicking on the link or responding to the request for information.

To protect yourself, keep the following in mind:

Just because a message appears to come from a friend or someone you know does not mean the message is safe.

Cyber criminals may have infected their computer, hacked their account or spoofed their From address.

If you are suspicious about a message from someone you know, call the person to verify if it was truly them who sent it.

Be suspicious of any email directed to "Dear Customer" or some other generic salutation.

Be skeptical of any message that requires "immediate action", creates a sense of urgency or threatens to shut down your account.

Be suspicious of messages that claim to be from an official organization but have grammar or spelling mistakes.

Most organizations have professional writers and do not make these mistakes.

Before you click on a link, hover your mouse over it, this will display the true destination of where you would go.

Confirm that the destination displayed matches the destination in the email and is going to the organization's legitimate website.

Even better is to type the website into your browser.

For example, if you get an email from your bank asking you to update your bank account, do not click on the link.

Instead, type your bank's website in your browser, then login to the website directly.

Be careful with attachments; only open attachments you were expecting.

Basic Security I – How to protect

Cyber criminals can send you infected attachments that can potentially bypass your anti-virus.

Using email and Instant Messaging safely is ultimately about common sense.

If a message sounds suspicious or too good to be true, it is most likely an attack.

Simply delete the message.

If you get a message and you are not sure if it is an attack, contact your help desk or information security team.

Browsers

Browsers are one of the primary ways we interact with the Internet, such as reading the news, shopping online or downloading files.

Browsers are also one of the most dangerous applications you use because they provide an entry point into your computer.

Cyber criminals know this and as a result have developed techniques for attacking your browser.

A common technique cyber criminals will use is to create tools that attack and exploit your browser, then place these attack tools on websites.

When you visit these websites these malicious tools silently probe your browser and launch multiple attacks.

If your browser is vulnerable, the attack will give cyber criminals control of not only your browser but potentially your entire computer, with no indication this occurred.

Unfortunately there is no simple way to tell if a website is safe or malicious.

Even legitimate sites can be compromised and used to attack you.

However, most modern browsers offer some protection.

Most modern browsers maintain a list of known malicious websites, these are evil websites that intend to cause you harm.

If you accidently visit one of these known malicious websites, your browser will post a warning, as you see here.

If you browser warns you against visiting a website, be sure you do not connect to it.

In addition, when you download and install or run a new program, that program may be infected.

It may appear to work as expected but could also attempt to silently infect your computer.

A key step to protecting yourself is to ensure that your anti-virus is actively scanning any new files you download from the Internet.

Finally, there are some other steps you can take to protect your browser and yourself.

First, use the most current version of your browser and be sure it is always updated.

This protects you from attackers exploiting known weaknesses in your browser and is one of the most effective ways to protect yourself.

Second, do not install plugins or add-ons into your browser unless you absolutely need them, they simply add more vulnerabilities for attackers to hack into.

If you do have plugins installed in your browser, make sure you keep them updated.

Just like your browser, you protect yourself by always using the latest version

Finally, some browsers allow you to set specific security settings.

You may want to consider configuring your security settings to a higher level.

While it might stop some legitimate sites from working, it will go a long way in keeping your system secure.

Mobile Devices

Mobile devices, such as smartphones and tablets, have become incredibly powerful.

Not only can you call anyone in the world, but you can watch movies, read your email, bank online and even install apps.

These combinations of factors make mobile devices very useful, however it also can put you at great risk.

To protect yourself, we recommend the following:

Just like with your computer, install only apps that you need and make sure that you download them from trusted sources.

Basic Security I – How to protect

Criminals can create apps that look real, but are actually malicious programs designed to quietly take control of your devices.

In addition do not install apps that request excessive permissions, such as the ability to silently send text messages or copy your address book.

Just like with your computer, backup your mobile device on a regular basis.

This way, if something happens to the device, your information is not lost.

Make sure you update your mobile device and apps on a regular basis.

Cyber attackers can more easily exploit your devices if you are running outdated software.

If your mobile device is old and no longer supported, consider purchasing a new one that can support the latest version of the operating system and security updates.

Never jailbreak or hack your own mobile device.

Not only may your device no longer be supported, but this usually cripples or disables many of the security features designed to protect you and your information.

If you have security software installed, such as anti-virus or a firewall, then make sure they are enabled and updated with the latest version.

Remember that many of the attacks you find in email can also happen via texting on your mobile device.

For example, cyber criminals can text messages asking you to connect to malicious websites, download infected apps, or ask you for private information such as your bank account.

If a text message seems suspicious or too good to be true, simply delete it.

Be careful when using Wi-Fi.

Many mobile devices will automatically connect to Wi-Fi networks without asking you, putting your device at risk.

Disable Wi-Fi if you are not using it.

Attackers can also take advantage of your Bluetooth capabilities.

Just like Wi-Fi, disable Bluetooth when you are not using it.

It is also important to turn off Bluetooth discoverable mode features.

Basic Security I – How to protect

Do not access or store work email or other data from our organization on your mobile device unless you have been authorized to do so and the appropriate security safeguards are in place.

Finally, when you lose a mobile device anyone can access all of your information including your emails, pictures or contact lists, unless it is protected.

Protect your devices with a hard to-guess password or PIN.

If your device supports encryption, we recommend you use it.

Also, consider enabling remote wiping if available.

This means if your mobile device is lost or stolen, you can erase all your information remotely.

If you lose a device issued to you by our organization or a device that contained any organizational information, notify the help desk or information security team immediately.

Passwords

Once someone knows your password, they can steal your identity or access all of your personal information.

Let's learn what makes a good password and how to use them securely.

There are two key points to good passwords:

First, you want passwords that are hard to guess.

This means do not use simple passwords such as 123456, your pet's name or your birth date.

Second, use passwords that are easy to remember.

If you keep forgetting your passwords they are not very helpful.

The problem is cyber criminals have developed sophisticated programs that can guess, or brute force your passwords, and they are constantly getting better at it.

This means they can break into your accounts if your passwords are not strong enough.

To protect yourself, you want your password to be as long as possible.

The longer your password is, the stronger it is.

In fact, instead of using just a single word as your password, use multiple words.

This is called a passphrase.

For example, your passphrase could be something simple like:

Time for chocolate!

To make your passphrase even more secure, do the following:

Use a number in your passphrase.

Have at least one lower case and one upper case letter in your passphrase.

Use a symbol in your passphrase.

Let's take our passphrase and make it even more secure by replacing some of the letters with numbers and symbols, as we just discussed.

First, notice how at least one of the words starts with a capital letter.

Then we can replace letters with numbers or symbols.

For example, you can replace the letter 'a' with the '@' symbol or replace the letter 'o' with the number zero.

In addition, we can add symbols using common punctuation such as spaces, a question mark or an exclamation point.

As a result, we now have a strong password that is very difficult for cyber criminals to compromise, yet is simple to remember and easy to type.

In addition to strong passwords, you must protect how you use them:

Be sure to use different passwords for different accounts.

For example, never use the passwords for your work or bank accounts for your personal accounts, such as Facebook, YouTube or Twitter.

This way, if one of your passwords is hacked, the other accounts are still safe.

If you have too many passwords to remember, consider using a password manager.

This is a special program you run on your computer that securely stores all your passwords for you.

The only passwords you need to remember are the ones to your computer and the password manager program.

Basic Security I – How to protect

Check with your supervisor, the help desk or the information security team to see if a password manager is an option you can use.

Never share your password with anyone else, including fellow employees.

Remember, your password is a secret; if anyone else knows your password it is no longer secure.

Do not use public computers, such as those at hotels or libraries, to log into a work or bank account.

Since anyone can use these computers, they may be infected with malicious code that captures all your keystrokes.

Only log in to your work or bank accounts on trusted computers or mobile devices you control.

If you accidently share your password with someone else, or believe your password may have been compromised or stolen, be sure to change it immediately.

Be careful of websites that require you to answer personal questions.

These questions are used if you forget your password and need to reset it.

The problem is the answers to these questions can often be found on the Internet, or even your Facebook page.

Make sure that if you answer personal questions you use only information that is not publicly known.

Many online accounts offer something called two-factor authentication, or two-step verification.

This is where you need more than just your password to log in, such as codes sent to your smartphone.

When possible, always use these stronger methods for authentication.

Finally, if you are no longer using an account, be sure to disable or delete it.