Cybersecurity Guidelines

For Employees

Q1 2020

What is Cybersecurity?

Cybersecurity is the process by which individuals and companies protect their digital assets from unauthorized access, use, disclosure, destruction, modification, or disruption. Digital assets include personal identity, data, emails, social media, websites, as well as hardware (computers, tablets, phones, networks, etc.).

Protecting your digital assets, whether personal or work related, has become an absolute necessity. For companies, it is critical to maintain trust with customers, remain compliant with the law, and maintain the company's image and reputation.

Some security measures may seem expensive, but it's nothing compared to what *not* having them will cost in the event of a breach. Think of them as an insurance policy, and insurance is only expensive *before* an incident.

Why Cybersecurity?

In today's digital world, there are so many potential security risks that it is increasingly important for individuals and companies to take steps to protect their digital assets, including their identity. That's where cybersecurity comes in. Some of the risks include:

- Identity theft
- Corporate espionage
- Malware (viruses, trojans, adware, phishing, ransomware, etc.)
- Network intrusions
- Misuse of data
- System failure
- Data corruption

- Lost or stolen equipment
- Disasters (both natural and man-made)

Keep in mind that a very large majority of incidents occur because someone opened an attachment, clicked on a link, or responded to a phishing attempt. And this is true for both individuals and companies alike. As a result, it is critical that people learn to protect themselves, both at home and at work.

Cybersecurity Tools

Today, no one can provide 100% computer security, unless computers are disconnected from all networks and placed in isolated lead lined rooms.

The goal is to mitigate risks as much as possible, which is done through the use of various tools to provide a layered security fabric, which can include:

- Physical security (security guards, keycard readers, entry keypads, etc.)
- Network Firewalls (preferably with Unified Threat Management or UTM)
- Software Firewalls (on both servers and workstations)
- Anti-virus/anti-malware software (on both servers and workstations)
- Email encryption and/or certificates
- Biometric user verification
- Encryption
- Backups (online, offline, and/or cloud)

But no amount of physical or technological tools will provide absolute protection, which is why user awareness is a critical component of the security fabric.

Cybersecurity Components

Many believe that cybersecurity is all about technology, but that's only *one* of the pieces as cybersecurity is really comprised of 3 components:

- People
- Processes
- Technology

A failure of any component puts the other components at risk!

People

As an employee, part of your job is to protect and secure your company's data and systems, but also its image and reputation (not to mention your own).

In addition, it is very important for employees to realize that in some circumstances, ***they may be personally legally liable*** for incidents or breaches.

Many companies have guidelines for avoiding incidents and for steps to take when an incident occurs, so the very first thing employees should do is get familiar with their company's information security policies.

The Golden Rule

Always remember the cybersecurity golden rule:

DON'T CLICK ON THINGS!!!

Received an email with a link? *DON'T CLICK ON IT!*

Received a pop-up while browsing inviting you to click on something? *DON'T CLICK ON IT!*

A lot of malware requires you to take some action in order to do its dirty work and often all it takes is 1 click! Make sure the links are clean before you click, and if you don't know, then just ***DON'T CLICK ON IT!***

If possible, get confirmation before clicking on something. And remember that hackers can sometimes take control and respond as someone else, so it's better *(and safer)* to get confirmation by phone than by email.

Security Awareness

Most security experts agree that one of the biggest security risks are users themselves and raising their awareness on security concerns can greatly reduce that risk. After all, having tools in place to help protect data does nothing for security if users don't know how to use those tools or are not aware of the potential risks.

And if your company doesn't have such guidelines, then use common sense and try to learn to:

- Use anti-virus/anti-malware software to scan files you receive via email or download from the Internet
- Recognize phishing attempts
- Recognize fake communications

Remember:

- Never open an attachment from someone you don't know.
- Never click on a link from someone you don't know.
- Never give your login details for anything to anyone (even your helpdesk).
- If you get an "urgent" pop-up message that your PC is infected or has issues, or that you are in trouble with a local, state, or federal government agency and the

message directs you to call a number for immediate support or service – It's a scam – DON'T CALL THAT NUMBER!

- If someone claims to be from a well-known company or government agency and requests you pay for something using cards (gift cards, prepaid VISA or Master Card, iTunes, Amazon, etc) – It's a scam – DON'T SEND THEM ANYTHING!
- If you receive an attachment or link from someone you know, check with them to make sure what they sent is legitimate ***before*** you click on it or open it (keep in mind their email may have been hacked, so it's best to ***call*** them).
- If someone contacts you claiming to be from your credit card company and asks you to confirm your complete credit card information, do not answer. If it's via telephone, hang up immediately. Your credit card company has your card numbers and will never ask you for your account details.

For any communication that looks unusual or that you're not sure about, do ***not*** click on any links or images, do ***not*** open any attachments, and do ***not*** respond. If your company has a security team or helpdesk, forward the communication to them for verification. If your company doesn't have a security team or helpdesk, then inform your management and just don't respond. If it's by email, delete it. If it's by telephone, hang up (you can always call the company back yourself to confirm if the request is legitimate and take appropriate action).

When it comes to information security, it is ***always*** better to be overly cautious than not enough.

Phishing

Phishing is the attempt to acquire sensitive information such as usernames, passwords, social security number, credit card details, and sometimes even money, by masquerading as a trustworthy entity in an electronic communication (email, social media, and even by telephone).

An example of phishing: an individual called employees of a company pretending to be part of that company's helpdesk and obtained login information from some employees, which he most likely would have used to hack into the company's systems. Fortunately, one employee contacted the helpdesk and found out it was a phishing attempt. The helpdesk immediately forced all employees to change their passwords before any damage was done.

Fake Communications

As mal-intended individuals and groups get more and more sophisticated, it's getting harder for people to detect fake communications.

When you get a communication that has several grammatical errors, there's a good chance it's fake and written by a foreigner.

Most email programs will show you the email address of the person that sent you the email when you hover over their name. If that's not the case, search your program's help function to find out how you can see the original email address of the person sending you the mail. Take the time to check them.

Just like Phishing, fake communications can come via a variety of electronic means (emails, social media, telephone, etc.).

An example of fake communications: a CEO of a company had his emails hacked. In his emails, the hackers found one sent to the finance manager with instructions to transfer funds. They duplicated the email, changing the amount and the target account to one of their own in a foreign country. The finance manager executed the transfer only to find out later that the CEO had never sent such an email. Had the finance manager known to check the original email address on the email, he would have seen that it was not from a real company email account. Alternatively, he could have simply called the CEO to confirm the transfer.

Examples of Mal-Intended Emails

If you get any emails such as those listed below, forward the email to your security team or helpdesk for verification, then delete it. If you don't have a security team or a helpdesk, then inform your management and immediately delete the email.

- Email from employees or senior management requesting you to send money or take action for the company. Always confirm or validate directly with the requestor by telephone to ensure they really are requesting you to take action for the Business.
- [MAILBOX IS 97% FULL] or [Alert ! : You Have 3 Undelivered Pending Mail]. These are fake emails.
- Court Cases / Legal notifications – "Hearing of your case in Court No#7385". No legitimate court would email such notifications or demands to appear.
- Microsoft Updates to your computer for Windows, Internet Explorer, Outlook, etc. Any updates should be performed by company tools, your helpdesk, or via Windows update, ***never*** via links in an email.
- Banks and credit card companies do not send out emails asking for their customers to validate their account

information. If you receive this type of message, this is clearly an identity theft scam.

- Email stating that you have a very rich, long lost relative that has died in a horrible accident while living in Nigeria. This is a scam asking you to forward bank account details so they can deposit the funds from that relative's will.
- Official looking customer complaints, often made to look like they are from agencies such as the BBB or credit agencies. These agencies send these in letter form and ***not*** emails. The messages usually contain an internet link or an attached document that contains a link to a website. They are intended to lure you to a website that will download a virus or malware to your computer.

We can't stress this enough: for any email you are not certain about, do ***not*** click on any links or images, do ***not*** open any attachments, and do ***not*** respond.

Passwords

Many companies implement Single Sign On (SSO) solutions, and many companies have rules for password complexity and duration, but few provide tools to help users manage passwords. So some users use simple passwords that are easy for them to remember (and often easy for others to guess or crack).

The best policy is to use different long complex passwords for each system or application, and to change them regularly. However, that makes it difficult for people to remember all their passwords.

That's where password managers can help. They store passwords in encrypted form and make them easily available,

so users don't have to remember them all. They just need to remember 1 password: the one to open their password file.

There are 2 types of password managers: those that store passwords in the cloud and those that store them locally. It's not a good idea to store your passwords on someone else's system or in the cloud. If they get hacked, then all your passwords would be at risk. It's better to use password managers that store their data locally.

Password managers such as Ilium eWallet or Keepass make it very simple for users to use unique complex passwords as they:

- Can open a web site or application and enter the user's id and password for many web sites or web-based applications.
- Can generate a unique complex password for every site or application.
- Store passwords in a local encrypted file
- Are simple to use

eWallet also makes it very easy to synchronize passwords between devices, including PCs, phones, and tablets.

Using multifactor authentication makes it extremely difficult to hack an account as it requires more than a user id and password to access an account. You must either have a special device (hardware token), a software token (an app on a smartphone), or some other way to confirm your credentials (i.e. text message, email, etc.).

There are many smartphone apps that provide soft tokens (Authy, Microsoft Authenticator, Google Authenticator, etc.) and they can be used on most major systems, including Microsoft, Google, Facebook, Amazon, etc.

Processes

Information Security Policies

Companies should create and maintain comprehensive information security policies that document:

- Security tools available and how to use them
- What to do in the event of an incident
- User password policies
- User access policies
- Email policies
- Use of printers, fax machines, plotters, and scanners (including their placement)
- Backup and restore policies, including instructions on how to backup and restore data when appropriate

If you don't know your company's information security policies or where you can find them, then check with your human resources department, your helpdesk, your technician, or your manager.

Audits

Companies should also plan regular audits to ensure company security policies are adequate.

If your company has such audits, take them seriously and cooperate with the auditors. They are not there to cause you trouble, but to help identify where your company can improve its cybersecurity tools and procedures.

Technology

Your company should have put in place various technologies to help mitigate some of the risks, but remember that no one can provide 100% security.

Firewalls

Firewalls are a critical component of any company's network security, as they are the 1st line of defense against network intrusions.

If you remotely access your company network, ask if two-factor authentication is enabled, and if so, learn how to use it.

Anti-virus/Anti-malware

Almost every anti-virus/anti-malware program allows you to run a manual scan, so anytime you get one or more files, either by downloading them or copying them from an external device, you should scan them for potential malware.

Learn how to use your company's anti-virus/anti-malware software to scan a single file or an entire directory.

Backups

Backups are a critical component of cybersecurity because when all else fails, they will be the only means by which computing systems will be returned to operational status.

Learn to back up your critical data.

Summary

Every week, mal-intended individuals or groups come up with new ways to try to get something they can use for gain.

Using tools your company puts at your disposal and learning about some of the risks and how to mitigate them will help you protect yourself and your employer. If you apply the same at home, they can also help protect you and your family.

What To Do When Malware Strikes

If your company does not have guidelines on what to do when malware is detected, then here are some steps you can follow to minimize both the risk and any damage:

1. Stop using the computer immediately and shut it down
2. Inform management, your helpdesk, and/or your security team
3. Isolate the computer from the main network - This can be done in a couple of ways:
    a. Re-configure the firewall so the computer is isolated from the rest of the network (usually done by a network engineer)
    b. Unplug the network cable from the computer
4. For viruses and malware *other than ransomware*, have a qualified technician:
    a. Backup any critical data
    b. Either run a full malware cleanup to remove any malware or rebuild the computer by wiping the hard drive(s) and re-installing all software
    c. If the computer was rebuilt, then:
        i. Scan data backed up to ensure it is virus free
        ii. Restore data to the computer
5. For ransomware, things can be a bit more complicated:
    a. Is a recent backup available? If so, determine how much data would be lost if you restored from the most recent backup. If the amount of

data lost is acceptable, then have a qualified technician:

i. Check backups to ensure ransomware is not present in the backups, and if it is, they'll need to take precautions so it is not restored
ii. Save any salvageable data on the computer
iii. Rebuild the computer by wiping the hard drive(s) and re-installing all software
iv. Restore your data from the most recent backup and any data that was saved

b. If no backup is available or the amount of data lost would be unacceptable, then determine the criticality of the data on the computer.

   If the data is critical, then your only option is to pay the ransom (in most cases, you will receive a decryption key, but keep in mind that there is no guarantee you will be given anything). If you go this route, then make sure you follow any instructions you're given to the letter, both for the payment of the ransom and for the decryption of your files.

   If the data is not critical, then have a qualified technician:

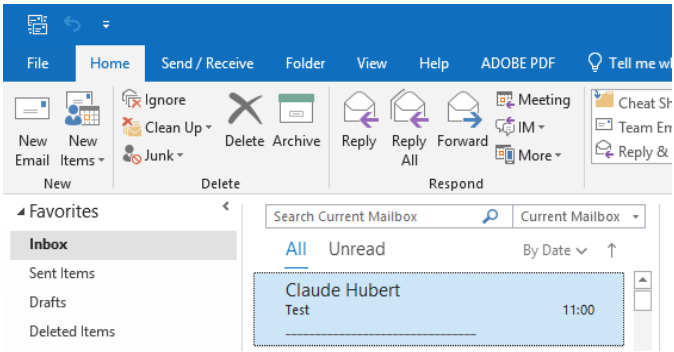
   i. Save any salvageable data
   ii. Rebuild the computer by wiping the hard drive(s) and re-installing all software
   iii. Restore any salvageable data that was saved

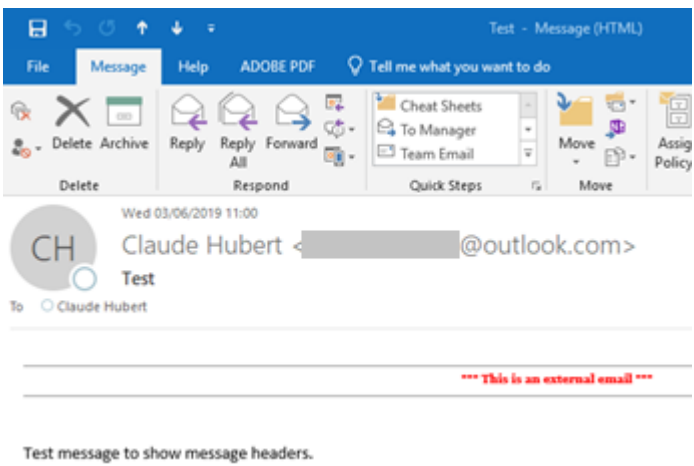
Checking Internet Headers in Outlook 2016

Internet headers contain information on the transport and origin of emails. You can check the headers to verify that an email is from who you think it is.

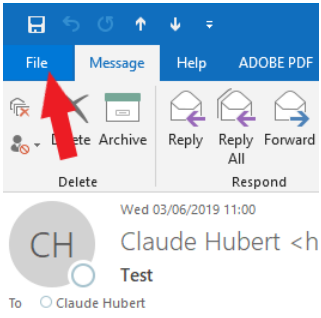
Be warned, checking Internet Headers is somewhat technical, but once you get the hang of it, it's easy and quick to do.

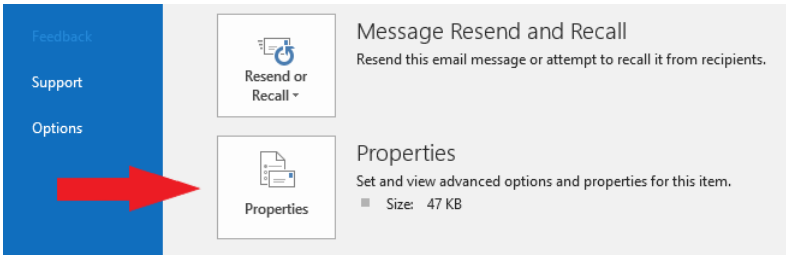
1. Open the message in outlook by double clicking on it.





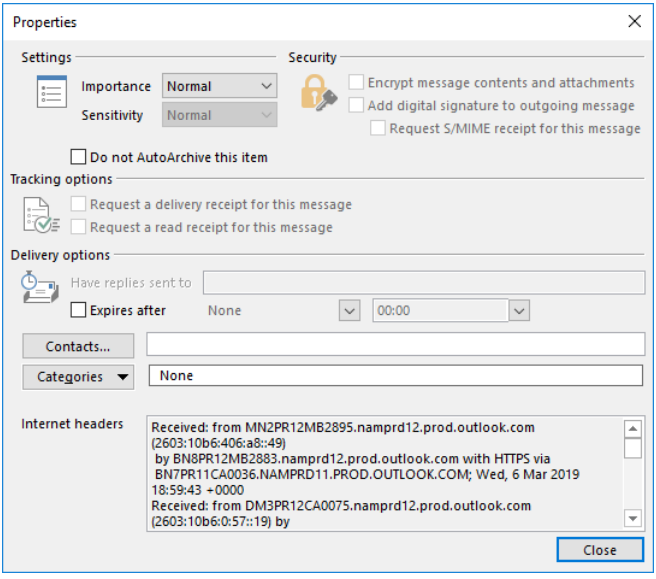
2. Click on File on the menu bar at the top, then click on the button [Properties].





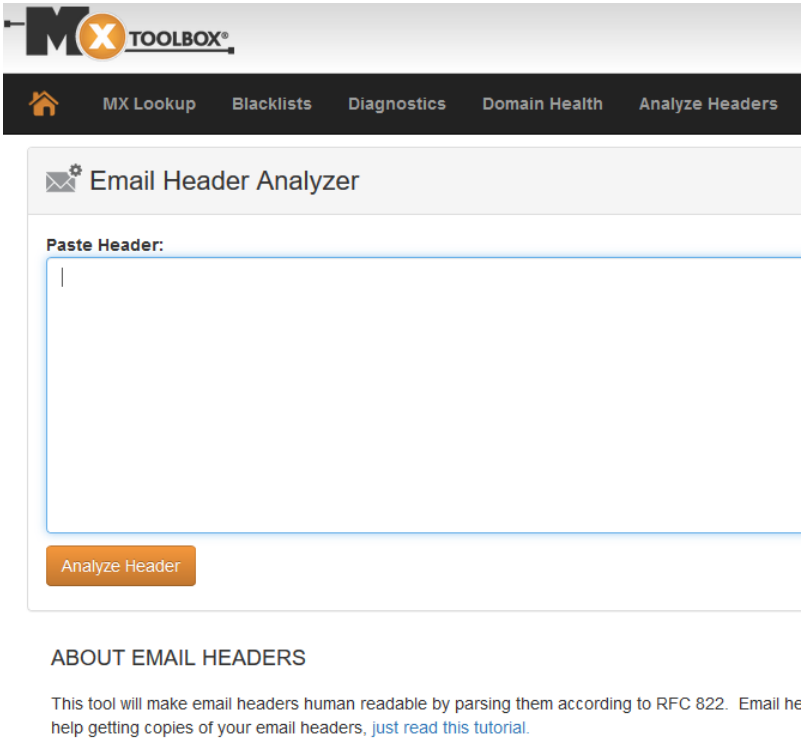
3. This will display the properties dialog window. The last item on that window is [Internet headers]. Click in that box and press [Ctrl-A] or right-click and click on [Select all] to select the entire contents, then [Ctrl-C] or right-

click and click on [Copy] to copy the contents onto the clipboard:

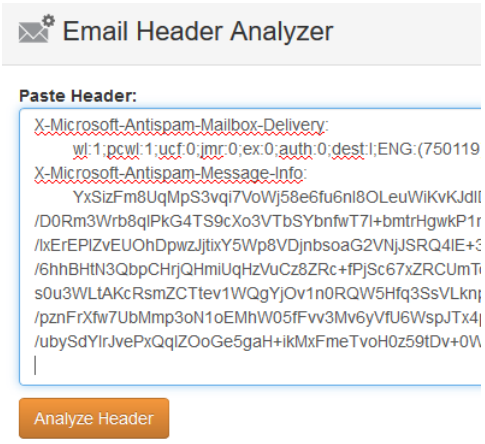


4. Open a web page and go to the following web site:

   https://mxtoolbox.com/EmailHeaders.aspx



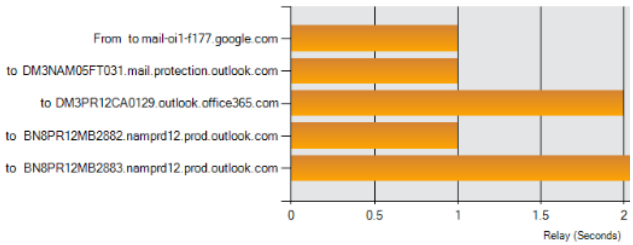
5. Click in the [Paste Header] box and press [Ctrl-V] or right click and click on [Paste] to paste the contents of the clipboard.



6. Click on the [Analyze Header] button – It will take a few seconds for it to analyze the headers.
7. The first thing to look at is the [Relay Information], which shows you the email servers the email was routed through. There's a graphic that shows you each of the servers and a bar to show how long it took to get through that server:

Relay Information

Received Delay:	**3 seconds**



Things to look for:

- If the email was sent from outlook or Office 365, then the 1st server listed should end in "outlook.com" or "office365.com"
- If the email was sent from Gmail, then the 1st server listed should end in "google.com"
- If the email was sent from Yahoo, then the 1st server listed should end in "yahoo.com"
- If the email was supposedly sent from the U.S., then the 1st server listed should end in ".com", ".org", or ".net".

If any of the above do not match what's expected, then it's most likely a forged email and you should be very careful.

8. Next thing to look at is the [Headers Found] section. There you should find the following entries:

From	Claude Hubert <[redacted]@gmail.com>
Date	Wed, 6 Mar 2019 14:05:16 -0800
Message-ID	<CAP0zaeKsQ+j8uA_QgGj4arhU7YuFek57PH44Oobe3JmxhJYmYA@mail.gmail.com>
Subject	Test
To	claude.hubert@tpx.com
Return-Path	[redacted]@gmail.com

Things to look for:

- The email addresses in [From] and [Return-Path] should match. If they don't, then it's potentially a forged email and you should be very careful.

You can follow these instructions to check older emails to see what servers you should be expecting for different people and if the email addresses match in the [Headers Found] section.

Last Updated
March 25, 2020

Version

2020Q1-0309