Sometimes it feels that the world of email and internet communication is fraught with dangers: malware, viruses, cyber attacks and so on.

There are some simple things that you can do to protect your email data and accounts. Let’s look at three of the most common and real threats and what you can do to safeguard against:

**Viruses and Malware**

**Non-Secure Communications**

**Data Loss/Leakage**
PASSWORDS

Let’s begin with the most important security tool available: passwords. This is nothing new. We all know that we should use strong, unique passwords for all of our email accounts. In fact, most of us are prompted to change our passwords regularly.

A strong password:
• Has at least 12 characters
• Includes numbers, symbols and both capital and lowercase letters
• Is not a dictionary word or combination of words
• Does not have obvious substitutions such as a zero in place of the letter “O”

Pro Tip: If you don’t already, it is a good idea to create a separate email account for your newsletters, subscriptions, etc. Keep this mass distribution email separate from your work and personal email accounts.

TWO-FACTOR AUTHENTICATION (2FA)

In today’s modern email world, you can add a second layer of safety to your account. Much like having two locks on your front door, you can implement 2FA for your email account. 2FA combines use of something you know, like a password, with something you have, like your mobile phone, a security token, a USB stick, etc.

When you turn on 2FA, your email application will send a code to your mobile phone. When you login to your email account, you must enter both your password and the code. This makes it nearly impossible for someone to hack your email account.

Here is an analogy: to use an ATM, you need your PIN (like a password) and your debit card (like a phone).
When using a work-related email account, your company likely has anti-spam and anti-virus software in place to protect you from email viruses. However, these software apps cannot prevent all malicious email, and some malicious threats come from the internet.

**Some malicious threats include:**
- Trojan horses
- Viruses
- Worms
- Spyware
- Phishing
- Ransomware

Besides using unique, strong passwords and 2FA for each of your email and user accounts, here are some of the most important things you can do to protect yourself from malicious email.

- Always keep your computer’s anti-virus software and browser software up-to-date. These applications are updated or patched frequently to address new threats.

- **Do not, ever:**
  - Open an email from an unknown address.
  - Click a link in an email unless you expected someone to send it.
  - Open an attachment unless you were expecting it or it was from an unquestionably trusted source. Scan any attachment before you open it!
Viruses and Malware

Threats from email and the internet

Most of us already follow these basic email safety rules, so why repeat them? Hacking of email accounts is so common that almost every day you can expect an email from someone you know that was sent as a result of a hack. So, even if you recognize the From address, you should not automatically trust the content in the email.

Here are two specific examples of malicious emails that you might believe are real:

1. **Spoofs:** These are emails with a forged “From” address. Maybe you receive an email from your company CEO or doctor’s office requesting some type of personal data. Any time an email requests personal data, assume it is malicious. Contact the sender via another method to confirm the request before sending anything like passwords, account numbers, credit card information, etc.

2. **Hacks:** A Yahoo! account was recently hacked, and everyone in the user’s contacts received this email:

   [Malicious link]. Isn’t it incredible? I am totally impressed!

   The text following the link looks like something the user would send to friends. Luckily, no one clicked the link, but some unsuspecting users might have.

**OTHER BEST PRACTICES**

Not all malicious threats come from email—many are from the internet, instant messages (IMs) and file-sharing sites. Here are some best practices to follow:

- Be careful and selective about what you download to your computer from the internet.
- Read licensing agreements carefully.
- Do not click on internet ads.
- Do not open or accept suspicious error messages in your browser.
- Do not click on IM links from users you do not know or if they are otherwise suspicious.

Doing any of the above actions can result in software downloads to your computer, and these downloads are often malicious.
There are levels of security when it comes to email. First, there is a secure email connection, and then there are secure, encrypted email messages.

SECURE EMAIL CONNECTIONS

How many different places do you check your email?

- **Work:** Your work network should be secure.
- **Home:** Whenever possible, use a hard-wired internet connection, which is the most secure. If you have to connect over WiFi, ensure that your home network is secured with WPA2 (WiFi protected access II).
- **On the Go:** If you are working on a public network, such as a coffee shop WiFi, this is probably not a secure connection, and your email can be intercepted. However, if you have a VPN (virtual private network) application running, that will keep your data safe on a public network.

The fastest way to see if your network connection is secure is to check the network settings or preferences on your computer. On a Mac, select **Open Network Preferences > Advanced**, and you can see the security setting for each of your preferred networks. “WPA2 Personal” means you have a secure connection.

You can also check the connection between your email provider and your computer for security. Look at the URL. If it begins with “https,” it is secure. If it is “http” (without the s), it is not. The “https” is also important for any website you are using to transmit sensitive data, such as credit card information.

The s represents either SSL (secure socket layer) or TSL (transport layer security) encryption.
Secure Communications
From SSL to Encryption

MAIL CLIENTS

A mail client is an application that you install and run on your computer/device. This is different from a webmail application (such as Gmail and Yahoo! Mail) that you access through your web browser. When using webmail, your data is stored in the cloud. Many people think that using a mail client is more secure than webmail. However, the most common security breaches happen between the user and the server.

To make your mail client communication secure:
• Use the latest version of your email client.
• Configure your email to use SSL and TLS for all your IMAP and POP3 configurations, and use Submission (587) MSA. This was built specifically to prevent massive outgoing attacks. Use SMTP if your email client and server support it, but SMTPS is also secure.

SECURE, ENCRYPTED EMAIL

Some industries have compliance requirements, and many customers expect their information to be private and secure. If you work in the medical or legal industries, you are likely already familiar with sending secure, encrypted email. Encrypted email cannot be read by anyone without the decryption (private) key, so it is safe if intercepted.

The most common email encryption protocols are PGP/ OpenPGP (Pretty Good Privacy) and S/MIME (Secure/ Multipurpose Internet Mail Extensions). Some email services have these encryption options built-in, but you can also download encryption software yourself.

VALIDATING TLS

If you want to validate that your email server is using TLS to transmit messages, you can check this in most email applications by viewing the header (right-click and select View original):

Return-Path: <jorge.delacruz@synacor.com>
Received: from smtp.corp.synacor.com (smtp.corp.synacor.com [69.168.102.214])
    by mx.google.com with ESMTPS id c75si1807045qkb.105.2017.01.13.10.33.42
    for <jorgedlcruz@gmail.com>
    (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
Fri, 13 Jan 2017 10:33:42 -0800 (PST)

The blue text above indicates that the message was encrypted during transport with 128 bits using a cipher based in SHA 256 bits.
HOW DOES ENCRYPTION SOFTWARE WORK?

After an initial set up on the email server, your web client uses modern, built-in encryption libraries in the web browser. The next steps depend on the technology being used.

**S/MIME:** The user needs to add a SSL Certificate that is generated and sent only to this user. This SSL can be protected with a password.

**PGP:** This process is a bit more complex. The user needs to generate a keypair. A keypair has a private key, which should be stored in a secure place, and a public key that is used to decrypt all messages sent with that private key. This is explained more below.

If you are using an email application with encryption functionality, you should be able to specify that all emails be encrypted, or you can select individual emails for encryption as needed when composing.

Initial set up of encryption software (usually done by your Mail Administrator) requires a security certificate from a CA (certified authority). This step ensures that a trusted company (the CA) verifies that your email address is the correct owner of a public key and a private key generated by the encryption software.

Your email contacts automatically receive the public key when you send them email. This is done transparently, in the background, and it is nearly instantaneous. Now, when you encrypt and send an email, your public key is attached. The recipient’s public key is exchanged with your key, and the email is decrypted. If the email is intercepted, it cannot be decrypted because the hacker will not have the corresponding key.
DATA LOSS/LEAKAGE PREVENTION (DLP)  
From SSL to Encryption

**LOSS OF PROPRIETARY INFORMATION**

Loss and/or leak of proprietary data is a major concern for businesses, so most companies have DLP filters that check both inbound and outbound email. These filters ensure that employees are compliant with any rules and regulations for their industry.

However, regardless of the industry in which you work, consider the content of your email and IM communications before clicking Send. Is the content something that should be shared outside of your company? When in doubt, ask before sending.

---

**THE BIG FINISH**

This paper started with scary words: danger, malware, viruses and cyber attacks. That was intentional, to catch your attention. If you have read through this long, you clearly understand that these issues are real, and now you know how to protect your data. Please use the Email and Internet Safety Checklist below to ensure that your data stays private, safe and secure.

---

**EMAIL AND INTERNET SAFETY CHECKLIST**

- [ ] Verify passwords are strong.
- [ ] Verify that each account has a unique, strong password.
- [ ] Enable 2FA for each email account.
- [ ] Regularly update anti-virus and browser software.
- [ ] Do not open email from unknown senders.
- [ ] Do not click on links in emails or IMs unless you are certain they are secure.
- [ ] Do not open attachments unless you have scanned them and know they are virus-free.
- [ ] Be careful and selective about what you download to your computer from the internet.
- [ ] Read licensing agreements carefully.
- [ ] Do not click on internet ads.
- [ ] Do not open or accept suspicious error messages in your browser.
- [ ] Encrypt your email communications when necessary.
- [ ] Use public WiFi connections with caution.
- [ ] Do not share proprietary company information.