Email Security: A Guide to Keeping Your Inbox Safe in 2019

By Jacob Roach – Deputy Editor
— Last Updated: 02 Nov'18 2018-11-02T00:06:12-08:00

As a trusted form of communication in which personal information is often shared, email is a prime target for attackers and interceptors. Banks, social media sites and hospitals all communicate over email, and sifting through what's legitimate and what's a scam can be difficult. In this guide to email security, we're going to go over the threats that you face while using email.

We'll talk about the scams lurking in your inbox as well as the potential vulnerabilities while sending files. We'll also cover the different types of encryption you can use on your emails and some additional tips on staying protected. If you're more a do-it-yourself type, check out our guide on how to encrypt emails.

The good news is that most web-based email clients encrypt your messages, and do a good job filtering through spam, too. However, it's still not the most secure method of communication, which may mean you'll have to move to another application if security is your focus.

Before we make suggestions, let's look at the threats email faces.

Email Threats

There are two main categories for email security: protecting against attacks and protecting against interception. First, we're going to talk about the threats to your inbox and how you can avoid falling victim to scams and fraud. We'll then move on to how to secure your messages in-transit so no sensitive information falls into the wrong hands.

Inbox Threats

The first batch of threats target your inbox. These aren't specific to email; an attacker could use any means of communication. Even so, email is a large target for phishing schemes, fraud and more.

Most modern email applications, such as Gmail, do a good job of protecting you from these schemes. It's important to respect the spam folder your email application has, as the rules applied to spam are continually getting stronger.

Phishing emails make up a large portion of emails filtered into spam. Phishing is some sort of fraudulent communication — in this case email — asking you to provide personal information, such as your bank account number and routing information.

As you can read about in our what is phishing guide, most of these threats are easy to spot, and your spam filter does a good job of getting rid of them. However, there are more crafty schemes that can get past your spam filter and scrap your account information.

A large phishing attack targeting Gmail users surfaced in 2017. Users would receive an email saying someone they know shared a Google Doc with them. Clicking on the link would bring you to a page where you choose the Google account to view the doc, which is ordinary for this process.

However, once you attempted to login, there was a verification process asking if "Google Docs" could access your account information. This was, of course, not the legitimate application but one built to look just like it. Clicking through allowed the attackers to access the personal information associated with a Google account.

Inbox based threats are delivery mechanisms for other fraudulent activity, such as installing malware on your machine or stealing account credentials. These threats can be aimed at the masses, but there are targeted phishing schemes, too, most of which are a result of man in the middle attacks.

Transit Threats

A man in the middle attack (MitM) is a form of eavesdropping in which a third-party spies on information passing between two parties. The name explains it all; there's someone in the middle of your communication, stealing what's passing between.

MitM attacks can lead to spear phishing, which is a targeted form of the scheme described above. An attacker can spy on a communication and use fake accounts to appear as if they were a contact of the targeted user.

For example, an attacker could spy on the network traffic of a CEO. The attacker could then fake an email to appear similar to one that the CEO was expecting, which would, of course, be fraudulent. The CEO clicks through, credentials are stolen and the attacker makes off with some important data.

There are two forms of MitM attacks. The traditional "man in the middle" is where an attacker sets their machine as a proxy between your connection. If you're sending an email to someone, it would first go through the attacker's machine.

This type of attack requires proximity to the victim. Someone on the other side of the world couldn't grab your internet connection and monitor what's passing through it. This is because MitM attacks rely on weak security in routers to spy on a network. This is one of the reasons there's so much danger in using public WiFi.

Attackers scan the router for any vulnerabilities it may have, then use to tools to intercept and read the transmitted data. In some cases, that means skimming emails as they're being sent and, in others, it means redirecting the victim to malicious websites.

There's a second form called man in the browser (MitB) attacks, which uses malware loaded on the users computer to compromise account or financial information. In the case of email, you can contract this malware through phishing attempts.

Types of Email Encryption

One way to protect emails is through encryption. Let's take a look at the most important types.

Transport Layer Encryption

The most common email encryption protocol is STARTTLS which, as the last three character imply, is encryption that happens in the transport layer. If both the sender and recipient are using applications that support encrypted communication, an eavesdropper cannot use a sniffer — a tool used for MitM eavesdropping — to spy on the communication.

STARTTLS is the most common encryption protocol used for email. As of October 2018, 92 percent of all inbound emails to Gmail are encrypted using it.

Unfortunately, support for a particular protocol doesn't mean an encrypted connection. In some cases, the two parties can't verify each other's certificates, which would cause the encrypted connection to fail. However, most email delivered over TLS uses opportunistic encryption, meaning it will revert to plaintext rather than fail.

Mandatory certificate verification isn't ideal for email, either, as it's likely that verification will fail and, thus, the email won't send. This would mean that some emails would send without a problem, others would take multiple attempts and some just wouldn't send at all.

This type of encryption takes place in the transport layer, meaning users don't need to do anything to encrypt or decrypt the communication. It's the same type of encryption that happens when you land on a site with SSL/TLS certification. You can learn more about that in our SSL vs. TLS guide.

It also means that the recipient can scan or filter the message before it's delivered.

There are some consequences for this form of encryption. Since the encryption happens between individual SMTP relays, the message can be viewed and altered while in-transit. Anyone who

has access to, for example, a business's email system could read and modify the email before it's delivered, bringing up the need for end-to-end encryption.

End-to-End Encryption

While TLS encryption happens in the transport layer, end-to-end encryption happens only at the ends of a communication. The sender's message is encrypted before being sent, and it's only decrypted once it's been delivered. End-to-end encryption means the message can't be read or modified by anyone while in-transit.

OpenPGP is a data encryption standard that provides end-users with the ability to encrypt email contents. It uses public/private key pairs, meaning the sender encrypts the message using the recipient's public key before sending it. You can learn more about this type of encryption in our description of encryption guide.

As with any more secure method of transit, there are issues with end-to-end encryption. In the case of OpenPGP, it's the public/private key pair. While this is considered a more secure form of encryption, it means that anyone who wants to send you an email would need to know your public key.

You'd need to establish the public/private key pairs beforehand and share it with anyone who wants to email you. For the majority of home users, it's an unnecessary and annoying process that will have negligible security benefits.

End-to-end encryption is a business-focused method of security. By establishing the key pairs with mainstay clients, a business can ensure that all communication is secured. B2B communications benefit, too, so long as the receiving server has access to the decryption keys.

Protecting Your Email

Encryption is largely based on what email provider you're using. Most browser-based clients, such as Gmail, are using TLS to send messages, which should be enough for an individual. Businesses may want to consider end-to-end encryption, but securing with TLS is a start.

You can test if your email service is using TLS by using a tool like CheckTLS. As you can see below, we tested Gmail, and all of the result were positive. All emails sent between these servers are encrypted with valid certificates.

Contrast that with the NSA mail servers, which encrypt emails but use outdated certificates.

If you're using Gmail or G Suite, you're covered on the TLS front, and you shouldn't have to configure any settings. If you're getting email from the best web hosting providers, you can often configure your encryption within your email settings. This is found in cPanel, an excellent web hosting interface featured in our best web hosting with cPanel guide.

Custom Filters

You can also set custom filters in most email applications that will work alongside your spam filters. Gmail is employed by the vast majority of users, so we'll walk you through setting custom filters there.

From your Gmail page, click on the gear icon in the right corner, then select "settings."

Once in your settings, click on "filters and blocked addresses" in the top menu.

On this page, you can import filters from other clients or create new ones. For this example, we'll create a new one by clicking on "create new filter" in the middle of the screen.

A window will open with a list of settings. You can filter messages from an address, emails that contain certain words, emails of a specified size and more. For this example, we're filtering emails that contain the word "dog."
Now, click on "create filter." Google will pull up results for all emails matching your filter settings, along with another settings box. This is where you can set how the filter reacts to emails that meet your criteria. In this example, we're going to choose to star all emails containing the word "dog."

Click "create filter," and you'll be brought back to the filter settings page. You can use filters to clean and categorize your inbox, but also to blacklist certain email addresses or sift through irrelevant messages.

Other Email Protections

You can setup different forms of encryption to increase your security. If you're a business owner, end-to-end encryption is likely your best bet, especially if you transmit sensitive information. For home users, there are a few things you can do besides simply emptying your spam folder.

Use a Password Manager

Online email clients are prime targets for data breaches. Yahoo reported in 2017 that somewhere in the neighborhood of three billion user accounts were compromised across email, Tumblr and Flickr.

Many passwords using the outdated MD5 hashing algorithm were stolen. If the attackers used a dictionary attack, or some other form of brute force, then those hashes could be translated into plaintext passwords.

We won't go into how that happens here, you can read our encryption guide, which is linked above, to learn more. Basically, a brute force attack relies on weak passwords for success. By guessing candidate passwords, an attacker can use software to match a particular hash to those candidate passwords, exposing the data.

Jeremi Gosney, CEO of Sagitta HPC, told Ars Technica that "any [passwords] with even a hint of complexity are pretty safe," though. As long as users had set a strong password on their account, a brute force attack on hashes is unlikely to work.

A password manager helps you do that. By generating strong, unique passwords for each of your online accounts, you can exponentially increase your security. Since brute force attacks rely on generating candidate passwords, a random bundle of letters, numbers and special characters is unlikely to come up.

It also gets past the problem of using the same password across your accounts. Providers such as Dashlane give you a security dashboard where you can monitor any weak or redundant passwords. It'll also notify you of any data breaches, as you can read about in our Dashlane review.

Password managers are one of the most practical ways to protect yourself from the dangers of cybercrime. You can read our best password manager guide or password manager reviews for recommendations, but we'll spoil it and let you know that we like Dashlane and 1Password the most.

You can see how those two stack up against each other in our Dashlane vs. 1Password comparison.

Install an Antivirus

Now that your account has been secured from data breaches, you need to protect against phishing schemes. For things that fall outside of common sense and your client's spam filter, an antivirus can protect you.

Antiviruses attack email threats from a few angles. The first is phishing protection. Bitdefender, for example, will actively scan web pages you land on for possible phishing attempts. First, it will search the URL for a match on a phishing blacklist. If the site isn't on the blacklist, it's considered approved.

However, that doesn't protect against the new onslaught of phishing pages that go up everyday. Phishing protection will look at the text, design template and more, then compare that to other phishing sites users have encountered. Because the structure of a phishing page has telltale signs, specifically sending the information to the attacker, this can usually snuff it out.

You can learn more about Bitdefender's phishing protection results in our Bitdefender review.

MitM attacks can be detected using a network analyzer, such as the one offered by Avast. This tool will analyze your network and all devices connected to it, as well as detail any vulnerabilities the network may have.

With that broad overview, you can see any suspicious devices connected to your network, too. It isn't a perfect protection solution, but it is a good sanity check, as you can read about in our Avast Pro review.

Much of the best antivirus software has business alternatives, too, many of which come with email server protection. Kaspersky, for example, has excellent security for mail servers. You can learn more about its consumer products in our Kaspersky Anti-Virus review.

Use an Encrypted Messaging App

The problem with email encryption is that you're forced to choose. For most users, setting up end-to-end encryption isn't feasible, as it would require all of your contacts to also set up encryption. If you're not content using TLS encryption, then you may want to cut communication via email and use a secure messaging app.

Private messaging apps deal with the headache of end-to-end encryption, providing you with a service that's as user friendly as sending a text message or email. Many applications also come with encrypted voice calls, self-destruct timers and private media galleries.

Keeper, one of our favorite password managers, includes KeeperChat with subscriptions. KeeperChat is a secure messaging application that includes a self-destruct timer, message retraction and more, as you can learn about in our Keeper review.

Other applications, such as the Signal Private Messenger, come with iOS and Android applications, as well as browser-based interfaces. Signal also has the benefit of being open-source, so you can find any vulnerabilities it may have by looking in the code or searching online.

While not a perfect solution, encrypted messaging applications are your best bet for highly sensitive information until end-to-end encryption becomes more widely used. The inherent problem with end-to-end is that both ends need to have it. Encrypted messaging applications deal with this issue and provide a secure way to send information.

Final Thoughts

Email security for home users is about as good as it's going to get for the time being. The majority of web-based clients use TLS to encrypt messages, which, unfortunately, comes with some downside. End-to-end encryption is a far more secure method of communication, but it's also difficult to set up for a single user.

Businesses, on the other hand, may be able to utilize end-to-end encryption in a meaningful way. If you're simply looking to secure your personal inbox, it's good to install an antivirus, use a

password manager and signup for an anonymous email service, such as TorGuard (read our TorGuard review).