Email Security Guide

BEST PRACTICES FOR SECURE EMAIL COMMUNICATIONS

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Information Technology | 202-994-4948 | ithelp@gwu.edu | https//it.gwu.edu

Table of Contents

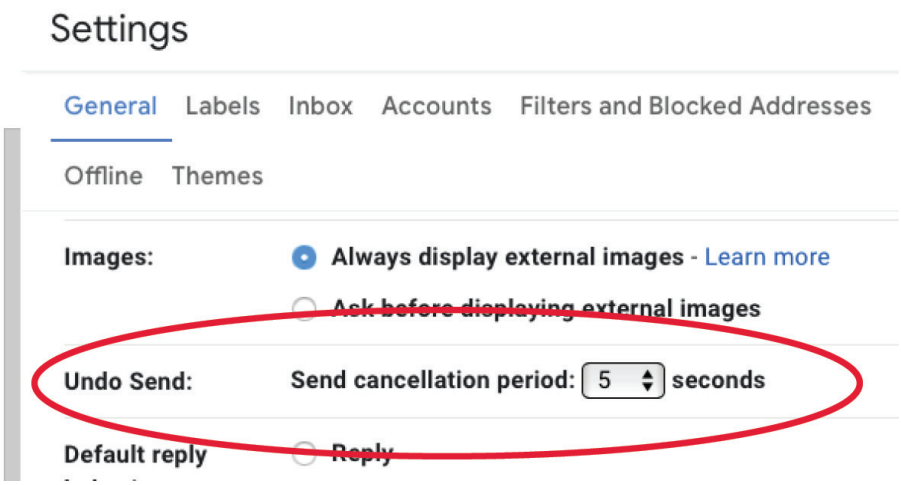
Responsible University Official:
TBD
Responsible Office:
Information Technology
Last Revised Date: November 26, 2018

Did you know that the first email was sent in 1971? It's true! Ray Tomlinson, a computer programmer, invented modern email by pioneering the "@" sign. As visionary as he was, Ray never foresaw how email would be abused, or the need for additional security for email messages. Today, there are over four billion email accounts and it is considered the most important and widely used communications medium on the Internet - all the more reason for increased email security awareness. Spam, phishing, and malicious attachments didn't exist in 1971, but these are all threats that must be considered when using email today.

Email was never designed to be secure; it was designed to work. As email use grew, especially in business, security features were added piece by piece. Email is still not inherently secure but there are things you can do as a user to optimize the security and privacy of your email account. The purpose of this guide is to walk you through steps to secure your email as well as introduce some basic email concepts and other good practices, especially if you regularly deal with non-public information. Non-public information can be regulated (data governed by local, state or federal laws) or restricted (data that should be shared in a limited way, such as payroll information or employee performance appraisals).

1) **Don't put anything in email that you wouldn't want in the newspaper.** This is just basic advice. When you send a message to someone you have a copy and they have a copy. At that point it is out of your hands. Because email is electronic, it's easy to retain emails for future reference. Sound judgment is required when composing an email message because chances are it will stick around for a long time. Further, email accounts can be compromised, allowing an unauthorized person to gain access to the contents of your inbox.

2) **Check email addresses before hitting send.** Many email addresses and names are similar so it is easy to accidentally send a message to the wrong person. Double check the email address and confirm a person's email address by checking the GW directory before you hit send. Recalling a sent email in GW email is not possible. Recall may be possible in Gmail for a short period of time after sending. If you use the Gmail web client, click the gear icon and select "Settings." Under the "General" menu, set the "Undo Send" setting to the cancellation period of your choice. Keep in mind this only works within the Gmail web client and will not work through a desktop email client such as Outlook.



3) **Check incoming email addresses before trusting a message or opening an attachment.** Scammers and phishers are smart and constantly change tactics to trick recipients into opening malicious attachments or triggering a response to their message. For example, take the message on the right.

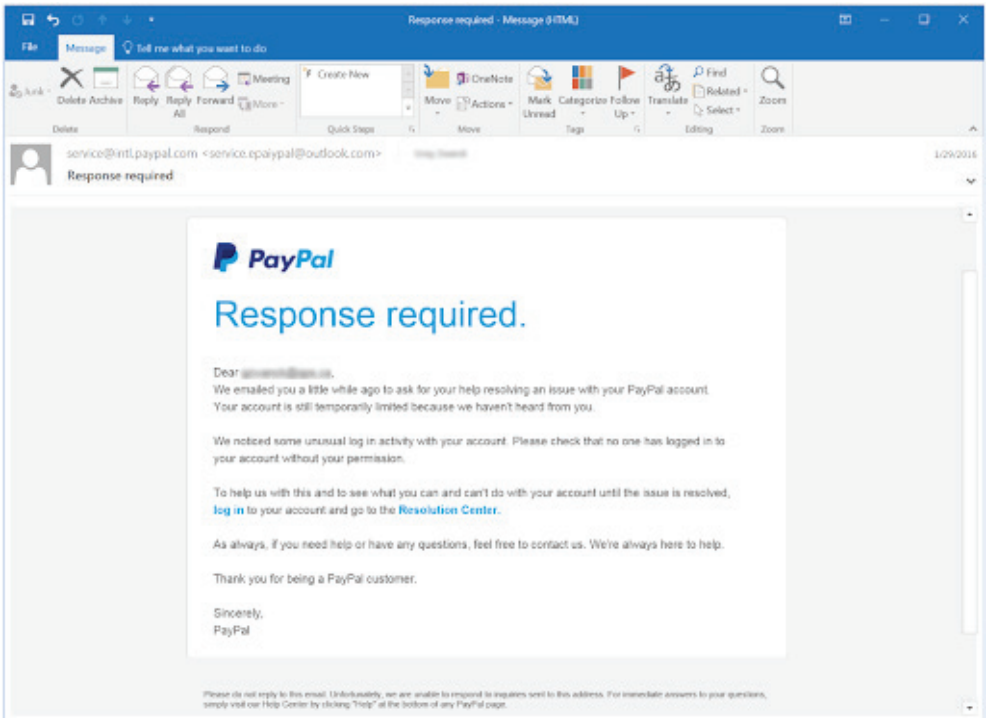
---------- Forwarded message ----------
From: **Thomas LeBlanc** <thomas.leblanc@[redacted]
Date: Tue, Nov 6, 2018 at 12:38 PM
Subject:
To: [redacted]

Are you free at the moment??
--
Best Regards,

If you just looked at the "From" line, you'd see that the message was from GW President Thomas LeBlanc. But if you looked at the sender's email address, you'd see that the domain (the part after the @ sign) was not gwu.edu. You have no way of knowing if this person is actually Thomas LeBlanc.

It is easy to create a phony account to pose as someone else in order to convince you to send wire transfers or divulge non-public information. If you're not sure or if something seems wrong, forward the message to abuse@gwu.edu and someone will review the message and get back to you.

4) **Don't take the bait.** Similar to #3, email scams, sometimes called "phishing" are techniques used by criminals and social engineers to trick a user via email. Phishing can take many forms and attackers are always changing their tactics. Let's take a look at an example of phishing:



In the example on the next page, the user has received an email urging them to take action on their PayPal account. Phishing and social engineering in general works because humans react to requests for compliance from trusted sources. If you were to click the "login" link, you would be taken to a page where you'd be asked to login to your PayPal account. That site will probably look a lot like paypal.com but it will actually be a fake login page. Once you login, the phisher will have your PayPal credentials. There are two ways to identify this message as a phish.

First, notice that the sender is "service.epaiypal [at] outlook.com." This is not an official message from paypal.com and further, "PayPal" has been spelled incorrectly.

Second, if you hover your mouse over the login link for a moment, you will be able to see the actual link. In this case, that link would not take you to the PayPal login page but to some other website not within the paypal.com domain.

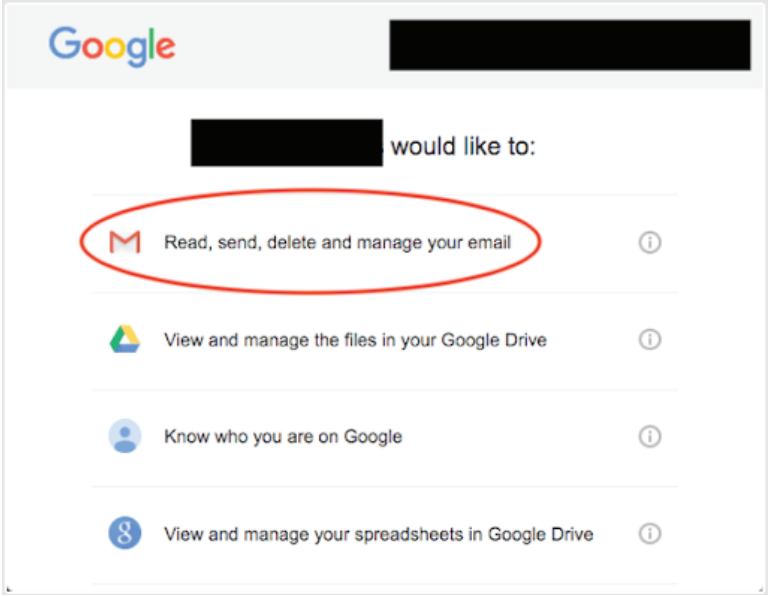
Keep in mind that phishing scams can come to you via email but also through LinkedIn, Facebook, and other communication platforms. It's a good practice to be mindful of these threats. Your account credentials and your data have value to an attacker and phishing is a low-cost, low effort way to get people to give the attacker what they want. This threat isn't going away anytime soon so it's up to all of us to be vigilant and report phishing when you see it. Report any messages that you think may be phishing to abuse@gwu.edu.

NOTE: The Division of IT will never ask you for your password over email or over the phone. The Division of IT, as well as other GW local support providers, do not need your password to troubleshoot your problem or provide you with technical support. Please keep your password to yourself and never share it with anyone.

5) **Don't put regulated data in email.** Regulated data is defined in the Information Security Policy as information that is protected by local, national, or international statute or regulation mandating certain restrictions. This can include personal information (such as a social security number or health information), credit card information, and student records. You should especially take care when sending data outside of GW. You are responsible for securely handling the data in your custody

   If you are sending non-public data outside of the university, use the Zixcorp email encryption service. This will allow you to send the message using a secure delivery mechanism by typing "encrypt" into the subject line of the email. Please note that typing "encrypt" into the subject line of emails sent from a gwu.edu address to another gwu.edu address does not provide any additional benefit. Contact ithelp@gwu.edu if you would like more information on how to take advantage of the Zixcorp encryption service.

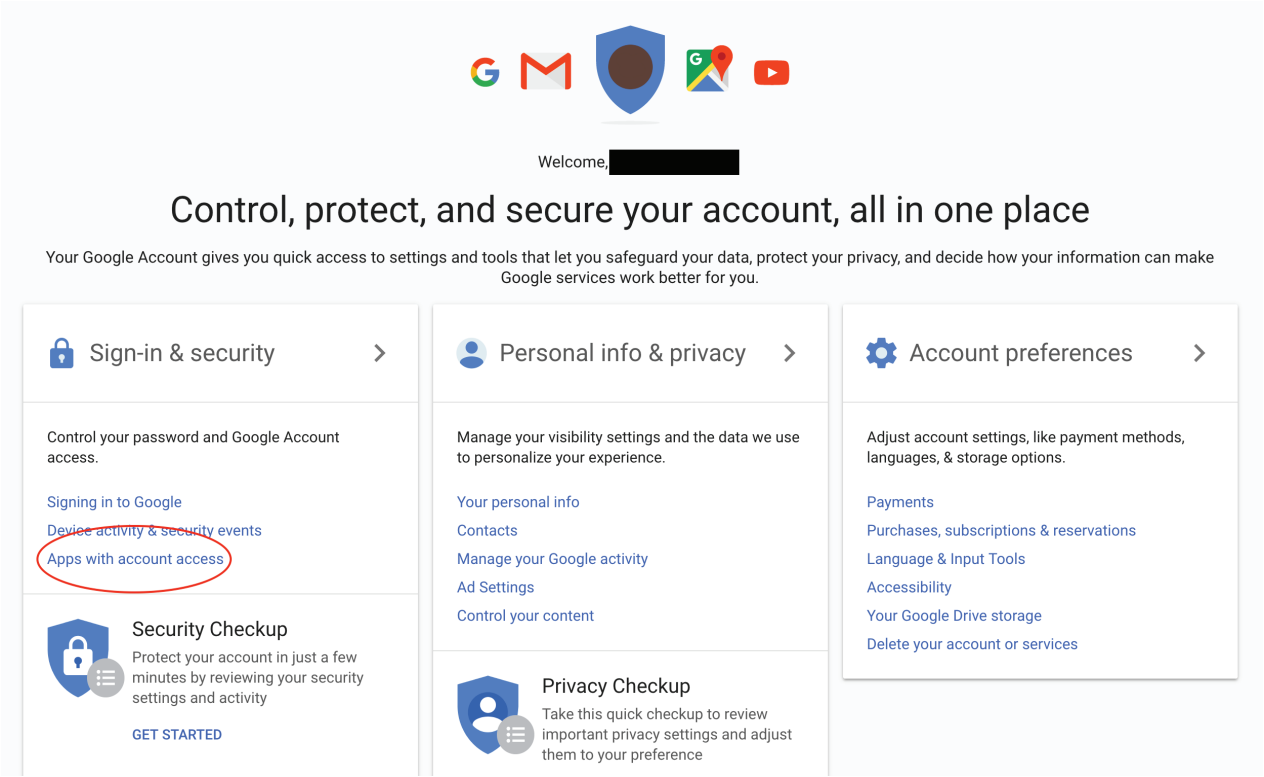
6) **Be wary of browser add-ons and applications that need to read your email.** If you've ever installed a browser add-on you may have seen a message that looks like this:



   Before you grant this kind of access to your inbox, think about the following questions:

   - Do I know and trust the developer of this add-on?
   - Do I know how they are using my email?
   - Is it appropriate for this application to be reading my email?
   - Is there non-public data in my inbox?

   In many cases, the answer to these questions will not support using this add-on. We understand that many add-ons are very helpful and provide useful functionality. This functionality comes at a price though and typically, that price is unfettered access to your private emails. Be mindful of this when granting this type of access. The application will continue to have this access even after you change your password. You can view all of the applications that you've granted access to by visiting this webpage: https://myaccount.google.com. Click "Apps with account access" to view which apps you've authorized to access your account. (See image on next page)



7) **Don't mix business with personal.** We strongly urge you to keep all official GW correspondence isolated to your gwu.edu email account. This means not using a personal or commercial email service to conduct GW business or forwarding your GW mail to a personal or commercial email account. It also means not using personally-owned or shared computers to access your email. As GW does not manage your personally owned computing devices, we cannot assist you with investigation and recovery should an email result in a security incident, malware, or data loss. GW-managed computers are configured to reduce the risks of email-borne threats.

Email is an important communication tool for the GW community. Your vigilance and awareness of these good practices will go a long way to preserve the confidentiality and privacy of non-public information at GW.

NOTE: Do not send regulated data through email. If someone is asking you to send regulated data over email, please contact the IT Support Center at ithelp@gwu.edu or 202-994-4948. If you are not sure if certain data is considered regulated, please visit https://compliance.gwu.edu/information-management and review the Information Security Policy and supporting documentation.

For additional information or help with any of these steps, contact the IT Support center at ithelp@gwu.edu or 202-994-4948.