What Happened? Why You Didn’t Receive an Email?

TTU email servers process a large volume of email every day. Occasionally you may receive a message that you were expecting or that someone indicated that they sent to you. Generally, the reason for not receiving an email would fall into one of these categories:

- The sender might have typed a typo in your email address.
- The message has been scored as spam by TechMail servers.
- Malware is attached that was detected by antivirus software – many times the sender may not be aware of the infection.
- The email has a “spoofed” email address (commonly used in “phishing” schemes).
- The message may be coming from a mail server that is generating huge volumes of spam mail; and/or

There might be a technical problem between the originating server and TTU mail servers.

One of the biggest culprits is the practice of “spoofing” email addresses. Internet criminals have exploited an Internet mail feature that allows a sender to supply an email address on the “From” line. When an email sender specifies an email address in the “From” line of the email that is different from his/her actual email address, the sender is “spoofing” or representing that the email came from a different email address. Unfortunately, Internet criminals quickly learned to leverage spoofing to conduct illegal activity and plant malware.

In this issue, we provide more detailed information about two strategies that we have deployed to defend against spam - SenderID and Reputation Filtering.

Using the Best-Of-Breed: TechMail Spam Filtering

On the server side, TechMail uses advanced methods to constantly monitor and scan all inbound and outbound email, scoring each individual email with a Spam Confidence Level (SCL). An email’s SCL is used by the email server to determine whether the email is delivered to the spam folders, junk, or email server to determine whether the email is delivered to the spam folders, junk, or email folder, or is rejected. Only emails with the very highest SCL score are rejected. The scoring algorithms are industry-standard and quite complex, and the exact logic is proprietary to the developers (for good reason, since spammers could easily devise ways to get around them if they had access to this logic). Emails between TechMail users are never scored as spam.

In the Outlook email client, additional options are available to help you recognize possible spam or unwanted email. By marking any individual email you receive as spam, Outlook will automatically place any future emails from the same sender in your Junk email folder. This effectively allows users to “blacklist” certain email addresses, or even entire email domains by adjusting Outlook’s options. “Whitelisting” is also supported, so that you can ensure receipt of emails from specific email addresses or email domains. Rules and Alerts are also available to help sort incoming email into appropriate folders. For a more detailed description of the client-side filtering options for Outlook and other supported TechMail clients, visit http://www.iitc.ttu.edu/info/spamfilter.php.

Beware of Rising Email Scams

Historically, any international disaster or media events cause an increase of email scams and threats. Spammers often use tragic events as opportunities to lure people into opening an alleged document or clicking on a link, only to discover that they have been tricked. Older emails may not be updated on a regular basis, increasing the risk of attackers exploiting your TechMail account.

A list of email campaigns, as well as setup instructions, can be found on IT Help Central's website at http://www.ttu.edu/techmail.php. TTU will not be able to provide support for non-recommended email clients.

Recommended Email Clients

TechMail is TTU’s email service. When accessing your TechMail account, you have a number of software options for your computer. TechMail can be accessed using Microsoft Outlook, as well as most email clients. Many of these clients were not designed to be used in a Microsoft Exchange environment and may not be able to take full advantage of the features that TechMail has to offer. Because of this, we strongly recommend following the recommended client options:

- Microsoft Outlook 2007/2010 (PC), or Outlook 2011 (Mac), or Outlook Web Access (https://mail.ttu.edu).

If you plan to use a third-party client to access your TechMail account, we recommend that you keep the following in mind:

- Most third-party clients connect to your mailbox only. They typically will not connect to your calendar, contacts, tasks, etc.
- These clients may require a VPN connection in order to access your TechMail.
- Integration with other TTU resources (Global Address List, Live Meeting, Communicator, etc.) from these clients is unsupported.
- Older email clients may not be updated on a regular basis, increasing the risk of attackers exploiting your TechMail account.

For a list of email campaigns, please visit http://www.ttu.edu/techmail.php.

Email has quickly become a primary means of communication in our digital world, with a majority of TTU faculty, staff, and students turning to email for communications once handled by phone, letter, or face-to-face meetings. While a simple method of communication for both the sender and recipient, email can be used for malicious purposes. To review guidelines for professional communication with email, please visit http://www.ttu.edu/safecomputing/ttu/etiquette.php.
Don’t Be the Bait for a Phishing Scheme

A phishing scheme occurs when thieves pose as legitimate financial institutions or companies through email to lure you into disclosing your personal information, such as your password or PIN number. When a TechMail account is compromised, criminals may use your account to distribute virulent attachments or spam. All too often this leads to Internet Service Providers across the world blocking all email from TechMail servers. The process of rectifying the situation consumes substantial university resources.

As a protection, when TTU security systems detect a possible phishing attack, the following warning message appears as the top of the identified email message:

"WARNING: This message is not from a sender on your Safe Sender's list AND MAY BE AN ATTEMPT TO STEAL YOUR PASSWORD. No email from a reputable source will ever ask for, or direct you to verify, your email account information! If you are certain of the sender's identity and need to reply or forward this message, delete this warning verbiage before sending and add the address to your Safe Sender's list. For further assistance, call (806)742-4357."

If you see this warning message in an email, you should exercise extreme caution before responding or clicking on any links within the message. If you know the email to be legitimate and you need to respond or forward the message, you must first remove the warning message, as TechMail will not deliver any email that contains the warning message.

Before this control was implemented, TechMail email servers were being blocked by external email providers regularly, as a result of TechMail users (including TTU faculty, staff, and students) responding to phishing schemes. Since adding this protection, we have drastically reduced these incidents. Note that TechMail will not insert the warning message if the email originates from an address contained in your Safe Senders list. If you are regularly receiving legitimate email that has the warning message, add the senders to your Safe Senders list to prevent these warnings from appearing.

Preventing Account Lockouts from your Wireless Device

Account locking is a common industry security practice that protects your account by preventing someone or a malicious application from guessing your password and gaining unauthorized access. Texas Tech University implements this security practice with your eRaider account. If an incorrect password is entered against your eRaider account too many times in a short time frame, your account will become temporarily locked. Since many TTU community members use handheld devices for accessing eRaider-protected services, it is important to remember to update your saved eRaider password on these devices when you change your eRaider password. These devices will continually attempt to connect to the network using your saved password, and if you have not updated your password, you will temporarily be locked out of your account and unable to access IT services.

In order to prevent account lockouts, the TTU IT Division reminds you to first disable your wireless connectivity, such as placing your device into “airplane mode”, or any similar feature which disables wireless. Once this is complete update your password in the following locations in your mobile device after changing your eRaider password (detailed instructions available online at http://www.depts.ttu.edu/ithelpcentral/info/passwords.php):

- TechMail (Settings → Mail, Contacts ...) Instructions available at http://www.ithc.ttu.edu/info/passwords/techmail_iphone.php
- Wireless (Settings → Wi-Fi) Instructions available at http://www.ithc.ttu.edu/info/passwords/wi_fi_iphone.php
- VPN (Settings → General → Network → VPN) If using VPN, instructions available at https://mail.ttu.edu

Also, best practice suggests that you reauthenticate your device after passwords have been updated in all locations on the device. Additional information about the eRaider account lockout policy may be found at www.depts.ttu.edu/ithelpcentral/solutions/EraiderLockOut.php.

Using TechMail on the Road

When traveling, you may need to access your TechMail mailbox. The TTU IT Division recommends the following steps to help ensure smooth TechMail access when you are away from your office:

- Before leaving, check your email client settings and verify that you can connect to your email from an off-campus location (instructions available online at http://www.ithc.ttu.edu/techmail.php);
- Familiarize yourself with Outlook Web Access (https://mail.ttu.edu). In the event that you cannot connect to your email client, Outlook Web Access is a viable alternative for accessing your TechMail account through a current browser;
- If your eRaider password is due to expire soon, consider changing it prior to your trip. You can check the status of your eRaider password online at https://eraider.ttu.edu;
- Before leaving, verify that your wired and wireless connections are fully functional on the computer you plan to take with you. If you have a mobile broadband card, verify before your trip that you can connect through it as well; and
- Have a second device as a back-up, if feasible.

Following these steps can significantly improve your TechMail experience when traveling.

* See the TechMail (or Not) for VPN article in this bulletin for additional information.