Avoiding Spam and Phishing Emails

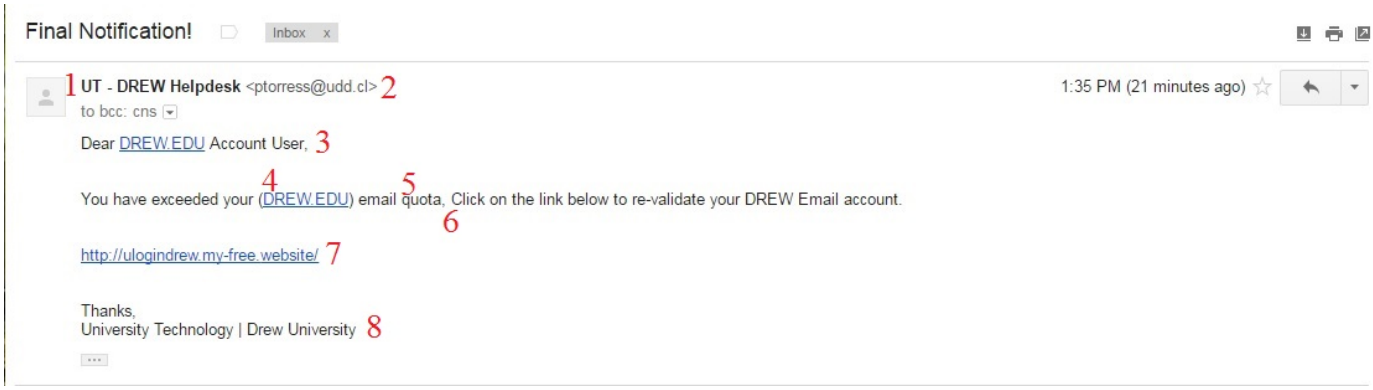
Click here to see an outline of this page.

Phishing Quiz

Can you spot when you're being phished? Take this quiz from Google and Jigsaw.

Sample Malicious Email

Here is an example of a malicious email message, and eight points that show you this is fake:



1. The Sender name does not match other emails from this sender.
2. The email address does not match the Sender name.
3. In this example, the email does not open in the same way other emails from this sender usually do (that is, with your name).
4. Why is the domain name in parentheses?
5. Your Drew email does not have a quota.
6. Typographical errors are often an indicator of spam or phishing emails.
7. The URL does not match typical Drew URL and is not secure (http - you should always look for https)
8. The signature does not match standard emails from this department.

If you are ever suspicious of an email, it is better that you NOT click on any links or follow any instructions in the email. Contact the person or department the email is reportedly from via a different means, such as by phone. If you are concerned about the security of your password, navigate to the page in question yourself - not by following any links in the email - and change your password.

Some Questions to Ask Yourself about A Suspicious Email

Although making the time to check details can seem impossible, try to take a minute to notice a few things.

- Does the name in the subject match the From: address?
- What does the To: address say?
- Are you listed in To: or in Bcc: (you should be in To:).
- As with most spam, check for extra typos.

Viewing a file that is shared with you should not prompt you to approve additional access. Always pay close attention to WHO is asking for WHAT access, and consider carefully whether they need it or not (this is true of the apps you install on your phone, as well!).

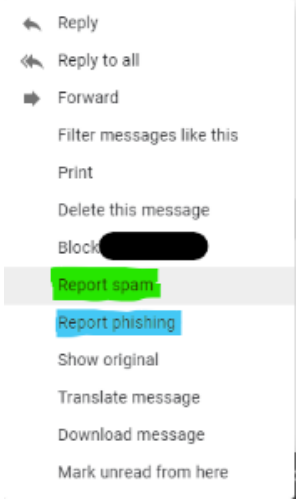
Steps to Take After Receiving Spam or Phishing Emails

As long as you have not clicked on any links or downloaded any attachments within a suspicious email, you can report it as spam or phishing and

safely delete the message.

Why report it? Because Google can use the data to better protect everyone. Enough reports received against a particular sender will prompt Google to block that sender.

1. Open the email.
2. Click on the 3 dot menu to the right of the email header (next to the time the message was received)
3. Choose "Report spam" (highlighted in green) or "Report phishing" (highlighted in blue)



But is it spam or a phish?

Spam is categorized as uninvited advertising - a message sent to large groups of people trying to convince them to buy a product or service.

Phishing is more targeted and more malicious. It is an attempt to garner personal information - often usernames and passwords - that can be sold and/or used to gain access to other information, systems, and/or money.

Was your account compromised?

If you think your account may have been compromised...

1. Change your password(s).
2. Consider running a virus scan.
3. Consider enabling multifactor authentication on your account (if you haven't already done so).
    a. Google offers a multifactor option at https://myaccount.google.com/security
    b. Drew offers Duo Security at drew.edu/duo
4. Check the following:
    a. In Gmail > Settings > Accounts and Import, look at "Check mail from other accounts" and "Grant access to your account".
    b. In Gmail > Settings > Filters and Blocked Addresses, look for any filters you do not recognize.
    c. In Gmail > Settings > Forwarding and POP/IMAP, check for any forwarding addresses.
    d. Visit https://myaccount.google.com/permissions to see what apps are connected to your Google account. Remove any you do not recognize (or no longer use).
    e. Visit https://myaccount.google.com/secureaccount to run a security check-up on your Google account.

Additional Examples, Resources and Information

- Please visit this article for additional examples and tips for recognizing phishing emails: https://www.bettercloud.com/monitor/c-suite-phishing-attack-examples/
- This Gizmodo article does a nice job of summarizing new phishing tactics (posted 3/20/2019): https://gizmodo.com/how-phishing-scams-are-evolving-and-how-not-to-get-caug-1832618224
- This article from How-To Geek tells you what you should and should not do with a phishing email: https://www.howtogeek.com/437513/what-should-you-do-if-you-receive-a-phishing-email/
- Password Safety Guidelines
- Best Practices For Keeping Your Computer Healthy
- StaySafeOnline.org article on Spam & Phishing
- SANS Cyber Security Awareness OUCH! Newsletter Archives
- USA Today article: 3 must-do steps to recover from a phishing scam
- Google Support article: I've been scammed