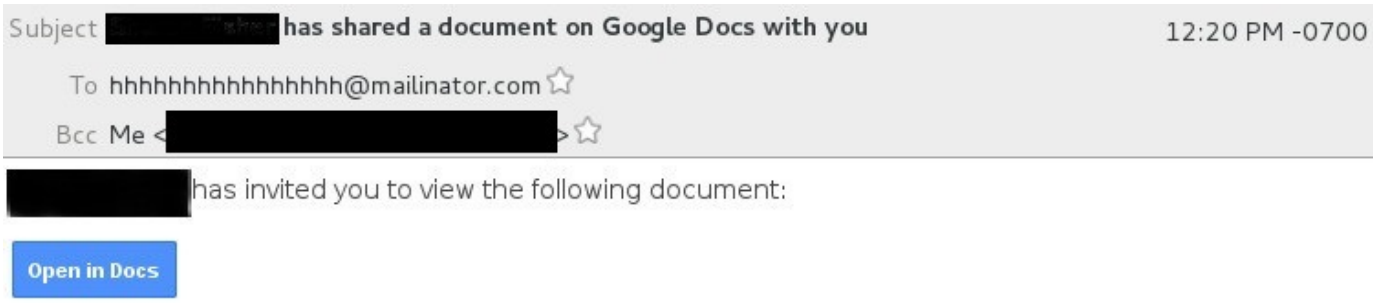
Someone shared a Google Doc with you?

And you weren't expecting it?

Try calling them to check.

How can we recognize phishing attacks?

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!).

Have You Been Phished?

There are a few things you should do if you think you've been phished.

1. Change your password.

2. 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
3. For a Google phish, 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 Resources

Password Safety Guidelines

Best Practices For Keeping Your Computer Healthy

StaySafeOnline.org article on Spam & Phishing

SANS Cyber Security Awareness OUCH! Newsletter Archives