

Good Morning and happy Tech Tip Tuesday (T^3)

Today's T^3 is dedicated to Spam and Phishing email. UGH

First some facts

- More than half of all spam falls into the following categories, in descending order by volume: health, adult, internet technology, personal finance and education.
- Spam isn't just an email nuisance. It can be found in virtually all electronic media including texts, blogs, phones, social media and search engines
- As of March 2018, the daily average volume of spam was 413.25 billion.
- The vast majority (85.2%) of all email is spam.

The above facts were pulled from Forbes.com - Apr 16, 2018

<https://www.forbes.com/sites/courtstroud/2018/04/16/on-spams-40th-birthday-25-things-you-didnt-know-about-junk-email/#4c43458a5c56>

Tips to recognizing Spam/Phishing email

1. The sender address isn't correct.

Check if this address matches the name of the sender and whether the domain of the company is correct. To see this, you have to make sure your email client displays the sender's email address and not just their display name. Sometimes you need to train hawk eyes at the address, since spammers have some convincing tricks up their sleeve. For example: From 'Joseph Monastero' <irr_1@icloud.com>

2. The sender doesn't seem to know the addressee.

Is the recipient name spelled out in the email, and are you being addressed as you would expect from the sender? Does the signature match how this sender would usually sign their mails to you? Your bank usually does not address you in generic ways like "Dear customer." If the email is legit and clearly intended for you, then they will use your full name.

3. Embedded links have weird URLs.

Always hover first over the links in the email. Do not click immediately. Does the destination URL match the destination site you would expect?

(Once again, train those eagle eyes.) Will it download a file? Are they using a link shortening service? When in doubt, if you have a shortcut to the site of the company sending you the email, use that method instead of clicking the link in the email.

4. The language, spelling, and grammar are “off.”

Is the email full of spelling errors, or does it look like someone used an online translation service to translate the mail to your language?

5. The content is bizarre or unbelievable.

If it is too good to be true, it probably isn't true. People with lost relatives that leave you huge estates or suitcases full of dollars in some far-away country are not as common as these scammers would have us believe. You can recognize when email spam is trying to phish for money by its promises to deliver great gain in return for a small investment. For historical reasons, we call this type of spam “Nigerian prince” or “419” spam.

Tips were pulled from Malwarebytes Labs - June 19, 2018

<https://blog.malwarebytes.com/101/2018/06/five-easy-ways-to-recognize-and-dispose-of-malicious-emails/>

When in doubt, call or send the NEW email to the sender.

Joe