Beware of Spam!

While some may be concerned about the iconic American meat that arrives in a rectangular 12-ounce tin (and is inexplicably popular in certain island states and American territories), more should be wary of its namesake – the spam that arrives digitally as email, text, and social media messages.[1]

The latter type of 'spam' took its name from the former. During the 1970s, Monty Python performed a sketch about a café that offered Spam in almost every dish, much to the dismay of a customer who didn't like Spam.[2, 3]

Half of email is spam

Most people who have encountered digital spam don't like it much, either. In fact, one cyber security company estimates spam comprised about 56 percent of all email traffic during the first quarter of 2017.[4]

Phishing is one type of spam. It occurs when cyber criminals send messages that promise untold wealth or attempt to steal (or persuade you to share) personal, account, or password data.[5]

There are variations on phishing, too. Criminals who 'spear phish' focus on specific targets. They gather data about individuals and then send one or more messages designed to get what they're after through 'social engineering.' *Symantec* wrote:[6]

> "The spear phisher thrives on familiarity. He knows your name, your email address, and at least a little about you. The salutation on the email message is likely to be personalized: 'Hi Bob' instead of 'Dear Sir.' The email may make reference to a 'mutual friend.' Or, to a recent online purchase you've made. Because the email seems to come from someone you know, you may be less vigilant and give the information they ask for. And, when it's a company you know asking for urgent action, you may be tempted to act before thinking."

Whale phishing generally targets high-profile executives or people with specific job titles. The goal is to convince them to disclose passwords or information that give criminals access to confidential information.[7] This year, a Lithuanian man was arrested after convincing employees at technology companies to transfer $100 million into accounts he controlled.[8]

We're all vulnerable

It can be extremely difficult to distinguish phishing scams from genuine digital messages. Often, phishing messages appear to be from reputable organizations or individuals, and it seems criminals refine their approaches every time the public learns how to protect itself.[9]

For instance, one tried-and-true method for identifying phishing scams was double checking a website's address and ensuring it had a padlock symbol indicating the site was secure. In April 2017, however, *Wired.com* reported that:[9]

> "A cunning new exploit makes malicious phishing websites appear to have the same URL as known and trusted destinations... a malicious site that can impersonate a legit

URL and depict that padlock leaves precious few tip-offs that you're dealing with an imposter."

If your mailbox is flooded with spam, that's a red flag, too, according to *CSOonline.com*. It may be a distraction designed to prevent you from recognizing "…fraudulent purchases and bank transactions made with your stolen identity and credentials."[10]

Use common sense

Since it's not easy to avoid technology, it's a good idea to become familiar with the basic steps you can take to protect yourself from phishing scams. The *Federal Trade Commission (FTC)* recommends:[11]

- Deleting email and text messages that ask you to confirm or provide personal information, account numbers, or Social Security numbers. Legitimate companies don't ask for this information via email or text.
- If the email contains a threat, be even more cautious.
- If you have doubts or questions, contact the individual or organization by phone.
- Don't reply to, click on links in, or dial phone numbers provided in the digital message.
- Use security software and set it to update automatically.
- Never email personal or financial information of any kind.
- Review your credit card and bank account statements as soon as you receive them.
- Think twice before opening attachments or downloading files. They may contain viruses or other malware.
- If you suspect an email is fraudulent, forward it to spam@uce.gov, and contact the organization or individual impersonated.

No matter how vigilant you become, you may fall victim to a scam. If you've been tricked by spam, there are steps you can take to minimize risks and seek justice. Visit the FTC website to learn more.

Sources:
[1] http://www.nbcnews.com/news/asian-america/80-years-old-spam-has-long-culinary-legacy-n779471
[2] http://www.nytimes.com/2005/03/12/theater/newsandfeatures/what-to-expect-of-spamalot-a-lot-of-spam.html
[3] https://en.wikipedia.org/wiki/Spam_(Monty_Python)
[4] https://securelist.com/spam-and-phishing-in-q1-2017/78221/
[5] https://www.irs.gov/uac/report-phishing
[6] https://us.norton.com/spear-phishing-scam-not-sport/article
[7] https://www.lifewire.com/what-is-whaling-2483605
[8] https://nakedsecurity.sophos.com/2017/03/24/man-charged-with-100m-whaling-attack-on-two-us-tech-giants/
[9] https://www.wired.com/2017/04/sneaky-exploit-allows-phishing-attacks-sites-look-secure/
[10] http://www.csoonline.com/article/2132829/access-control/flood-of-spam-email--it-may-be-a-screen-for-fraud.html
[11] https://www.consumer.ftc.gov/articles/0003-phishing