Wonderful Spam!

or: *How I Learned to Stop Worrying and Love the Spam*

Spam, Spam, Spam, Spam, Spam, Spam,
Lovely Spam! Wonderful Spam!

— The Vikings at the Green Midget Cafe
Monty Python's Flying Circus, 1970

Living With Spam

Junk email, or *Spam*, is detested by all who use email, with the exception of those who make a living from it. Spam is the most common form of social engineering—attempting to trick us all into giving up enough information to access our accounts and assets, either by phishing for our login credentials, enticing us to help some cash-poor multi-millionaire, or installing malware that scoops up our passwords or extorts us with ransomware. Spam's ultimate target is our money.

I have a few simple guidelines for dealing with all email without even worrying about Spam.

But first, let's answer that age-old question: *what is Spam really made of?*

Spam comes in several flavors with many ingredients: phishing and spear-phishing, spoofing, boobytrapped attachments, fake links, phony phone numbers or email-reply addresses, and bogus unsubscribe buttons. Let's sample them one at a time.

Phishing

Phishing usually tries to lure you to a fake login page to trick you into entering your real credentials for some account. Because you will be on the hacker's webpage rather than the real website, any credentials you enter will be captured by hackers for their own use later at the real site. With phishing emails being sent to thousands or even millions of addresses, some percentage of the recipients do fall for it and give away their account information.

Spear-phishing

Spear-phishing is a more targeted approach, usually aimed at a small group — sometimes just one person, a *whale* — whose account is especially valuable due to their position as a bank manager, system administrator, department head, accountant, or anyone with a higher degree of access to a system than the average person. Spear-phishing emails are often carefully crafted, incorporating researched personal information to be more believable. Though more work, the payoff from spear-phishing can be access to an entire system of accounts rather than just the account of the one person who was fooled. One *harpooned whale* can expose all of the accounts at a business, bank, retirement fund, or all of Twitter's so-called "verified" accounts. (Spear-phishing may include emails, texts, and phone calls.)

Spoofing

Spoofing is a common side dish with Spam. It is simply the custom-encoding of an email message so that it appears to come from a different address than the one that actually sent it. Two common types of spoofing are:

- Business Name Spoofing — where email appears to come from a place that you already deal with, such as a specific bank or from Apple Support.
- Contact Spoofing — where the email appears to come from one of your regular contacts. This can happen when a hacker gets access to someone's Contacts or their Address Book containing your email address. You then receive emails appearing to be from that person who had you as a Contact. Once a spammer has someone's Contacts, they need not hack their email account — just spoof it.

The point of Spoofing is to get us to open, read, and respond to a Spam email as if it came from someone that we already know, trust, and expect to send us email.

Boobytrapped Attachments

Attachments can be boobytrapped to run programming scripts, connect to websites, or install malware when opened. Common types of rigged attachments include: PDFs, Microsoft Word docs, and image files, though there are many others.

Opening a boobytrapped attachment can trigger actions over which we have no further control, such as installing malware or running system-level scripts which give a hacker access to all of our disc content. When seasoned with Spoofing, Spam attachments may get opened based on trust in the apparent sender.

Fake URLs and Links

Phishing emails often include links or buttons purporting to take you to a login page for your account. Spam links often don't go where they say they will! Even when the visible URL spells out the full website path, that may not be the address it will go to if you click it (*i.e.*, try this link to www.apple.edu). Buttons and links are just a label that takes you wherever its maker wants you to land or that triggers an action like installing malware. Don't click stuff in suspicious emails.

Phone Numbers

Phone Numbers in emails may not have anything to do with the sender. Don't call them. If you need to phone someone in response to an email, go to your Contacts record for them and use their real phone number you previously stored. Spammers might actually look forward to getting your call — letting them grab your phone number to go with your email. Say it with me… *Spam* ***and*** *Robocalls!*

Email Addresses

Senders' emails and addresses within the body or signature lines of an email should not be used to reply to unverified senders. Responding to Spam can either:

1. Increase the Spam you receive because you responded to Spam, or
2. You might "reply" to a *spoofed* account, which didn't actually send it.

Don't reply to Spam unless you want even more Spam.

Unsubscribe Links

Unsubscribe options in Spam will not remove you from a Spam list; they may make you a *prime* Spam target by verifying that you both open and read Spam, making your email more valuable to hackers. Or, that *unsubscribe* button might trigger a malware installation. Never try to unsubscribe from Spam. You can't.

Email Triage

All incoming email can be immediately identified as 1 of 3 classes:

1. Obvious Spam — If it's obviously Spam, don't open it. Delete immediately.
2. Suspicious Emails — those you aren't sure whether to Open or Delete.

3. Trusted Emails — those you feel certain came from trusted contacts and are tempted to open without further thought.

Let's consider each group. We've already dealt with Obvious Spam — delete it. What about handling Suspicious or even Trusted emails?

Coping with a Suspicious Email

There are several precautions to take when you receive a suspicious, unsolicited, or unexpected email:

1. View only the Preview (the default list view in iPhone's Mail app).
2. If an email does open, don't click links or download or open attachments.
3. Determine whether or not you would act on this email *if it were legitimate*. This does not mean trying to figure out if it's legit or not, but rather, *if you could assume it was legit*, would you take any action in response to it?
4. If you *would* act, use Safari Bookmarks or Favorites, or a website URL in Contacts or your password manager to go to the official website to log in. Don't use buttons or links in email. When done, move or delete the email.
5. If you *would not* act on it even if it were legit, move or delete immediately.

Dealing with Trusted Email

There are also steps to take when you receive email you assume is perfectly legit:

- The same steps listed above for Suspicious Emails — **yes, exactly the same**.

Always consider these questions before treating any email differently than Spam:

- Did I expect to hear from this sender? If it's predictable, is it on schedule?
- Does it look, feel, or sound like past communications from this sender?
- Does my Mail App recognize this sender as one of my Contacts?
- Do I want to read it?

If you answer enough of those questions **YES** to still feel confident about it, then do whatever you're comfortable with. For instance:

- If a trusted contact regularly sends links to news, jokes, or to an online meeting you'd like to attend, follow their links when you feel it's appropriate.
- If *Apple Inc*. sends a receipt for your monthly iCloud storage payment, or for a Music or App Store purchase, file it in an appropriate mailbox (not your inbox).
- If Apple Support surprises you with email urging you to login to your Apple ID due to recent iCloud problems, refer back to *Coping with a Suspicious Email*. Login to Apple's site from a *saved bookmark* to check that all is okay.
- If your bank emails that your monthly statement is ready and provides a button to view it, go back to *Coping with a Suspicious Email*. Use that bookmark you saved in Safari or Contacts to open the bank's official login webpage to see your statement instead of trusting an email button. If you haven't saved that bookmark yet, do a web search and bookmark the official login page for later.

Spam-Free and Loving It

Not needing to identify all Spam is liberating. I can triage all email without having to decide if some of it might be Spam because that won't affect how I deal with it.

Only two questions matter:

1. **Would I act on this email if it were legit**?
   If **yes**, take that action without using links or buttons in the email.
   If **no**, move on to Question 2.
2. **Would I save this email if it were legit**?
   If **yes**, file it in an appropriate mailbox. If **no**, delete it right away.

You do not have to decide whether or not you *think* any email is Spam or legit.
It doesn't matter because you won't rely on stuff in that email even if you act on it.

Most email can be deleted or filed immediately. Either way, it's out of your inbox, and you're done.

PREPARED FOR MY FRIENDS AT ALAMEDA MUG & IPHONE WITHOUT TEARS
AUGUST 2020