How Do I SPAM Thee…

President, Ministry Business Services, Inc.
Reprinted from *MinistryTech Magazine*

SPAM email can be dangerous and painful to the recipient and to any data they have access to. Whether it's ransomware, phishing, pushing of malware, or impersonation, a strategy is needed to protect ourselves. I'll address these different types of SPAM, and how each should be strategically managed.

SPAM Comes in Many Flavors
In addition to what many think is a tasty lunchmeat, SPAM also refers to unsolicited email, and those emails are usually intended to do the recipient harm. Sometimes the pain is small, but often it is big and costly. The most costly to an organization are usually ransomware and business email compromise; the most costly to an individual are usually phishing scams.

Here are some categories of email SPAM and how to respond to them:

- Business Email Compromise (BEC), a.k.a. Impersonation Emails
    - Form: These SPAM emails used to only target businesses working with foreign suppliers and businesses who use financial wire transfer methodology. But in the last year we have seen many occurrences hit churches and ministries using checks! The form of the attack, as it affects churches and ministries, is usually an email supposedly from a pastor or executive in the organization directing the recipient to immediately transfer funds or cut a check. These attacks are usually well researched (we are welcoming and friendly environments, and we give them all of our staff structure and names on our websites!), and can feel legitimate.
    - What To Do: Never comply with the request. Always, require a live voice confirmation of the request in person or via live telephone call.
- Ransomware
    - Form: Ransomware is malware installed on your computer that usually gets introduced through a SPAM email, compromised website, or even through a bot (internet program) that looks for Remote Desktop Protocol vulnerabilities. Once infected with the ransomware malware, data is encrypted and held for ransom.
    - What To Do: One of the best defenses against ransomware is to keep multiple days (we prefer a full month) of full data backups so your system can be 'reset' if an infection gets through your defenses. In addition to ensuring good backups:
        1. Never click on a link or graphic in an email you weren't expecting. Even if it came from someone you know, do not click any links. If you think the email and its links may be legitimate and want to click them– before clicking on them– hover your mouse pointer over the link without clicking. Doing so should show the destination of the link. I recently did this on an email I received from Microsoft that looked legitimate, but the link would have taken me to a *very* different location than

what I expected. Best rule: if you're not sure that it's okay to click, do not click!

2. Make certain your computer has a good anti-malware program running on it. That's true whether you're using a Windows or a MacOS computer. The solution my firm recommends is www.thirtyseven4.com… doing so will help prevent you from accessing most compromised websites.

- Phishing
  - Form: Phishing has a few forms, almost all of which happen through email SPAM. Phishing is the attempt to get the recipient to provide personal information about themselves that could be used to accomplish some form of identity theft. Phishing is sometimes referred to as *clone phishing* (a previously legitimate email that has been recreated with malware embedded or in links and re-sent to the same list of recipients as the original), *whaling* (phishing attacks aimed at executives and high-profile targets), and *spear phishing* (attacks targeting specific individuals that may even contain information about them discovered through websites, social media, and other sources.
  - What To Do: Never respond to a request for personally identifying information in an email without first confirming the source. I even take this a step further if I get a phone call from my bank about possible fraudulent activity in my credit card account! In the call they ask for my password to prove I am who they intended to reach. I decline their request and tell the caller *they* need to tell me my password to prove they are who they say they are since they initiated the call! They're not allowed to tell me, of course, so that's when I disconnect and call the number on my credit card– that way I know I'm talking to my bank.

These are a few SPAM categories. It is imperative that every organization use a high-quality SPAM filter on its email server to eliminate most of the SPAM from being delivered to email account holders. There are a lot of SPAM filter solutions available; our favorite is from Barracuda. They are the gold standard and best-of-breed in that industry.

Just an fyi… we host SPAM filtering for churches and ministries nationwide using a Barracuda SPAM Filter 600. We process more than 90,000 emails daily, and it blocks about 80%. That means about 80% of the email pointed toward your email inbox is unwanted! And some of it is dangerous!

Using a solid SPAM filter won't stop all SPAM from getting to users' email inboxes, but doing so will stop almost all of it. That reduces the likelihood that someone will click on something they shouldn't. But the best protection will only come from repeated training to all team members. I recommend reminding the team of the danger on a monthly basis during all-staff meetings. And if you know a story in which an organization was hurt as a result of SPAM, tell the story! Doing so will help those who don't take threats and threat-mitigation seriously to re-consider.