First Bank & Trust Company
Member FDIC

Volume 4, Issue 11

November 2018

It's Almost 2019
and Yes, SPAM is Still a Problem

INSIDE THIS ISSUE:

Member FDIC EQUAL HOUSING LENDER

Abingdon Virginia, East
276-628-3838

Abingdon Virginia, West
276-628-9558

Bridgewater Virginia
540-828-2020

Bristol Virginia, East
276-466-9222

Bristol Virginia, West
276-669-1122

Bristol Tennessee, Volunteer Pkwy
423-652-2022

Christiansburg Virginia
540-260-9060

Fairlawn Virginia
540-633-3793

Gray Tennessee
423-467-9966

Harrisonburg Virginia
540-434-0671

Johnson City Tennessee
423-975-9900

Kingsport Tennessee
423-246-3700

Lebanon Virginia, East
276-889-3401

Lebanon Virginia, West
276-889-4622

Lynchburg Virginia
434-455-0888

Norton Virginia
276-679-7401

Staunton Virginia
540-885-8000

Verona Virginia
540-248-7700

Waynesboro Virginia
540-943-5020

Wise Virginia
276-328-3439

Wytheville Virginia
276-228-1125

We are fast approaching 2019 and yes, SPAM is still a major nuisance for many. The worst thing to see when you open up your Outlook, Gmail or Yahoo! account is hundreds and hundreds of spam emails. They are unwanted, unwarranted and just downright annoying. With all the advancements in email filters you would think this would be one less thing we all have to worry about in the new digital era, but unfortunately spam continues to be one of the biggest issues and is a major security risk to you and your PC.

Research shows spam accounts for almost forty five percent of all emails sent. That is literally billions of spam emails being sent around the world! Majority of the spam are advertisements and many are from hackers. Trying to decipher between what is coming from a legitimate business and a bad actor gets a little tricky. Hackers are notorious for making emails seem like something they are not. For example many hackers have been able to clone the sites and verbiage of major corporations making it nearly impossible for most to tell a fake email from a real one. The United States takes the crown for the worst country for spam with Apple IDs being the most targeted corporation according to The Human Factor report produced by Proofpoint in 2017.

Make no mistake, spamming is a lucrative business and provides incentives, especially to hackers. With the billions of spam emails being sent globally there is bound to be some emails that get through filters and even the most vigilant computer user.

There are some basic steps you can take to help protect yourself from unwanted spam.

- ***Use your junk mail email filter.*** Microsoft Office provides a filter that automatically evaluates in-coming messages and sends those identified as spam to the Junk E-mail folder. Most free email providers also have the same option.

- ***Limit the places where you post your e-mail ad-dress.*** Public websites, such as newsgroups, chat rooms, bulletin boards, and social media increase your chances of being spammed.

- ***Always be careful when giving to charity via an email request.*** Unfortunately, some spammers prey on your good-will. If you receive an e-mail appeal from a charity, treat it as spam. If the charity is one that you want to support, locate their telephone number or Website to find out how you can make a contribution.

- ***DON'T ever reply to spam emails,*** not even to unsubscribe from a mailing list, unless you know with all certainty the sender is a trusted source.

- ***When shopping online, watch out for check boxes that are preselected.*** Companies sometimes add a check box that is already selected, which indicates that you give the company permission to sell or give your e-mail address to other businesses (or "third parties"). Clear this check box so that your e-mail address is not shared.

Sources:
https://www.propellercrm.com/blog/email-spam-statistics

Is it Time to Revisit Your Company Security Policy?

Every day there are countless victims of data breaches. One of the first steps in protecting your organization is the use of a strong Information Security Policy. Does your organization have a formal Information Security Policy? Not a "word of mouth, everyone is on the same page" approach, but a written document that is presented to new employees as part of their hiring package. When was the last time it was updated? Are employees required to sign the document annually?

Requiring newly hired employees to attest that they will follow your policies, and by implementing an annual information security policy review and re-authorization with your current employees, you are communicating how critical information security is to your organization. While it may take thirty minutes to update the policy and some time tracking your employees down and collecting their signatures, these steps play a crucial role in protecting your business and speak ten times louder than simple verbal admonishments about the importance of information security.

A security policy is crucial because it outlines the assets you need to protect, the threats to those assets and the rules and controls for protecting them and your business.

Technology is ever changing, therefore your security policy should reflect the changes that impact your organization.

Below are a few suggestions to consider when revisiting your security policy. Remember, the policy is not a one size fits all and should be geared towards your specific business needs.

⇒ Define what can (and cannot) be installed on computers.
⇒ Discuss password complexity. Underscore the necessity to keep individual passwords private by not sharing with others.
⇒ Determine what constitutes as private information that should never be shared outside the organization.
⇒ Have a process to deal with security-related events, how they should this be handled and who it should be reported to.
⇒ Have email standards.
⇒ Provide guidelines to deal with handling of sensitive data.
⇒ Determine what is acceptable use of devices and online materials.
⇒ Determine how and what sensitive data should be stored.

Sources:
https://www.zdnet.com/article/10-ways-to-develop-cybersecurity-policies-and-best-practices/
https://www.opswat.com/blog/10-things-include-your-employee-cyber-security-policy