Member FDIC EQUAL HOUSING LENDER

First Bank & Trust Company
The Bank That Puts You First
Member FDIC

July 2017 Volume 3 Issue 7

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

In this issue:

Web Browsers
Which One is Right for You?

Long ago, Microsoft Internet Explorer was the only web browser available. Today, there are many more options; ones that are faster, safer and more user-friendly. All internet browsers primarily have the same duty: to render HTML in multiple tabs or separate windows and allow users to bookmark pages. But behind the scenes, the similarity ends, with different operational duties and different features. Below are some characteristics of the top three browsers that may help you decide which one is right for you!

Mozilla Firefox

Mozilla Firefox is a free web browser and is completely open source. Since its introduction in 2002, it has made some changes, one of the biggest being its ability to customize the web browser to your liking, down to extremely specific details. Privacy and security is another big factor that draws many people to this web browser. Firefox goes to great lengths to protect your private information. The browser automatically blocks ads and trackers that collect data without permission. In addition, if using their privacy browsing feature, Firefox automatically deletes cookies and passwords from your computer, a huge plus in today's world of cyber-hacking .

Google Chrome

Chrome, operated by Google, is extremely popular and is known for its extraordinary speed. Chrome allows for multiple tabs to be opened at the same time, so if one site is slow to download, you can easily open another tab or window to continue browsing. One of the biggest advantages of Chrome is that it is not likely to crash. Every tab and window runs on its own, therefore one faulty site won't affect anything else that you have open. This feature also adds a layer of security by separating each site and application within a limited environment. Chrome is also known for its user-friendly abilities, with a design that is easy to navigate. It simplifies web searching by using URLs or just words or phrases to search for what you need. Another nice feature of Chrome is its ability to allow you to drag and drop tabs into existing windows to combine them.

Continue on page 2

Microsoft Internet Explorer

Microsoft Internet Explorer (IE) is one of the most widely used browsers, mainly because it comes pre-installed with most Windows operating systems. Although it is the most used, it has been said by many to be the least liked. One of the biggest complaints about Internet Explorer is its speed. In the age of fast connections, those extra few seconds for a page to download can seem like an eternity. Another drawback that has been reported about Internet Explorer is its lack of security. With that said, Microsoft has been working diligently on improving security. For example, Internet Explorer now has the ability for you to block sites from cataloging your browsing habits which helps prevent against phishing and malware attacks.

In the end, although all web browsers do somewhat of the same thing, they all bring something unique to the table. Like most products, web browsers will continue to advance. Whether it is their security features or allowing you to customize the browser to your liking, be sure to do your own research to see which web browser suits your needs best.

Sources:
http://www.pcmag.com/article2/0,2817,1815833,00.asp
http://www.techradar.com/news/software/applications/best-browser-which-should-you-be-using-932466
http://articles.centennialarts.com/comparison-on-all-major-web-browsers-internet-explorer-safari-firefox-and-google-chrome/

DMARC – How to Control Unauthorized Use of Your Business' Domain Name

There is nothing more important than a company's domain name. That domain name ties right into a company's identity, having a unique IP address that identifies who they are on the Web. As such, no company wants that domain name to be compromised by a cyber attacker. This can be devastating to a company.

Domain name hijacking, the act of changing the registration of a domain name without the permission of its original registrant, is not a new concept and these types of attacks have grown along with spoofing.

Over the past couple of years spoofing attacks on legitimate domain names have increased by 45%. Hackers have found spoofing emails to be one of the easiest and most profitable ways to infiltrate networks. Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. Email spoofing is a tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate source. The spoofed email sometimes displays the legitimate email address, but the return address is different and concealed behind the legitimate email account. Imagine your domain name being used to send spam emails about pharmaceuticals, real estate, or even health insurance when your business has nothing to do with those industries. But because the domain name is one that is known and trusted by the recipients of those spoofed emails, many of them may inadvertently open the email not realizing the danger.

Continue on page 3

Once hackers successfully infiltrate a network, there is no limit to the damage they could do. It is imperative that businesses have some type of defense in place to protect them from these types of attacks.

One such defense is DMARC (Domain-based Message Authentication, Reporting & Conformance). DMARC is an email-validation system. It is designed to detect and prevent email spoofing and is intended to combat certain techniques often used in phishing and email spam . DMARC ensures that legitimate email is properly authenticating against established DKIM ((Domain Keys Identified Mail) and SPF (Sender Policy Framework) standards, and that fraudulent activity appearing to come from domains under the organization's control (active sending domains, non-sending domains, and defensively registered domains) is blocked.

How it works: DMARC's alignment feature prevents spoofing of the "header from" address by:

1. Matching the "header from" domain name with the "envelope from" domain name used during an SPF check, and
2. Matching the "header from" domain name with the "d= domain name" in the DKIM signature.

Many large organizations such as American Express, Walmart, Wells Fargo, Bank of America and Apple use DMARC and have a published a DMARC policy. Companies such as PayPal have seen the benefits of DMARC and reported that the decrease in phishing attacks against their company is widely due to the increase of mailbox providers using DMARC.

Today 2.5 billion mailboxes worldwide are protected by DMARC and there has been a 45% increase in the number of domains that had a reject policy in place in 2015. Not only can DMARC prevent spoofed email from entering an organization's network, but it can prevent others from spoofing that domain. It can also provide reporting on who is attempting to spoof that domain and the frequency of those spoofing attempts. DMARC can help protect a company's reputation as well as their customers. One of their ultimate goals is to significantly reduce the amount of successful phishing attacks against a domain name.

Cybercriminals have huge incentives for committing domain phishing attacks because the payout is so high and takes little effort on their part. DMARC is just another tool in the arsenal against these all too common attacks.

Sources:
https://blog.returnpath.com/how-to-explain-dmarc-in-plain-english/
https://dmarc.org/
https://sendgrid.com/blog/what-is-dmarc/