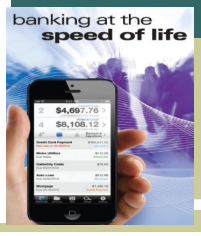
Mobile Banking App is HERE!



Volume 4, Issue 10

October 2018

HIDING IN PLAIN SIGHT

INSIDE THIS ISSUE:

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

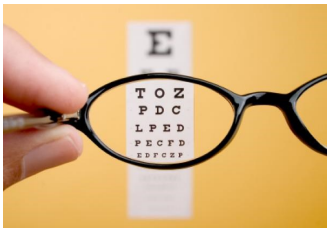
Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750 740-374-0010
This is not a full service location. Deposits/ withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967



There may be viruses and malware lurking around your PC and laptop that you are totally unaware of! As much as cyber security has enhanced and users are becoming more mindful, cybercriminals are now taking more of a back door approach, making themselves even more inconspicuous and hidden. Now, it's the silent attack that is becoming mainstream. Cybercriminals have been able to deploy very sophisticated attacks through viruses, ransomware and other malware by being incognito. The attackers strategically place in the background software that has the capability to record login keystrokes and track user behavior, thus allowing them to steal information, shut down networks and more.

One of these trends is spear phishing. Spear phishing is a form of email spoofing, however, the source appears to come from a trusted individual, many times from within the same company. What makes this type of phishing so successful are these characteristics:

- the source appears to be a known and trusted person,
- there is information within the message that helps support its validity, and
- the request the individual makes seems to have a logical basis and is within reason.

Another trend that is becoming more popular is hiding malware in trusted, well-known sites. If a site has a vulnerability, malware can automatically be downloaded to a PC without the visitor ever knowing. We all know that ensuring your antivirus is up to date is essential and helps catch many of these malicious attacks, but sometimes and unfortunately, it doesn't. The hackers have become savvy enough to know how the antivirus works and have created ways to bypass them. One way to try to stay protected is to educate yourself on the risks and to be aware of the hidden, non-traditional ways cyber-attacks are now being deployed. Below are a few unknown ways viruses can infect your computer without your knowledge.

⇒ ***On Line Ads***-We are bombarded with ads every day from all types of websites. Google analytics have made it extremely easy for advertisers to reach their target market. So when an ad pops up for something that piques your interest, don't just click right away; some of those ads can have malware hidden in them.

⇒ ***Social Media***- Studies show that more than three-quarters of all malware and computer viruses are entering computers by way of social media. People naturally trust social media because the messages are received from family, friends and familiar brands, which make a perfect platform for cyber criminals.

⇒ ***Mobile Malware***- Cyber criminals have been able to create apps that seem legitimate, but once downloaded, have the capability to steal information from mobile devices including banking credentials and other personal data.

Sources:
https://www.businessnewsdaily.com/6365-virus-nfections.html
https://abcnews.go.com/Business/YourMoney/story?id=8973

YOUR SSL CERTIFICATE IS IMPORTANT

What exactly is an SSL Certificate? SSL, better known as Secure Sockets Layer, is a digital certificate that authenticates the identity of a website and encrypts information sent to the server using SSL technology. The certificate serves as an electronic "passport" that establishes an online entity's credentials when doing business on the Web.

Recent studies have shown that ecommerce is growing faster than ever before. Most banks, in particular, allow their customers to do all types of transactions online, such as paying their bills or transferring money from one account to another. The certificate acts as a gate keeper. Anytime you transmit sensitive information, such as credit card numbers and personal information, the encryption provides a layer of protection that secures data being transmitted from prying eyes trying to do malicious activity. It helps prevent phishing attacks and provides authentication ensuring information is delivered to the correct server without being intercepted.

Having an SSL certificate provides your customers with a sense of trust and security. According to Gartner Research, nearly 70 percent of online users have terminated an online order because they did not "trust" the transaction. Many companies provide site seals and other images that indicate well-trusted encryption is in on their site. Displaying these branded icons gives customers an added level of assurance that their information is safe. This extra step will allow customers to breathe a sigh of relief knowing that an organization has done due diligence to try to protect them. Another way users know your site is safe is by recognizing the replacement of the “http” protocol with “https” along with a padlock image in the browser status.

It is absolutely worth the investment given the benefits of SSL certificates. Proper use of SSL certificates will not only help protect your customers, but it can also help protect you!

Sources:
https://www.sslshopper.com/why-ssl-the-purpose-of-using-ssl-certificates.html
https://www.forbes.com/sites/forbestechcouncil/2018/05/18/why-an-ssl-certificate-is-important-for-your-company-website/#a62a3fb1dc3e