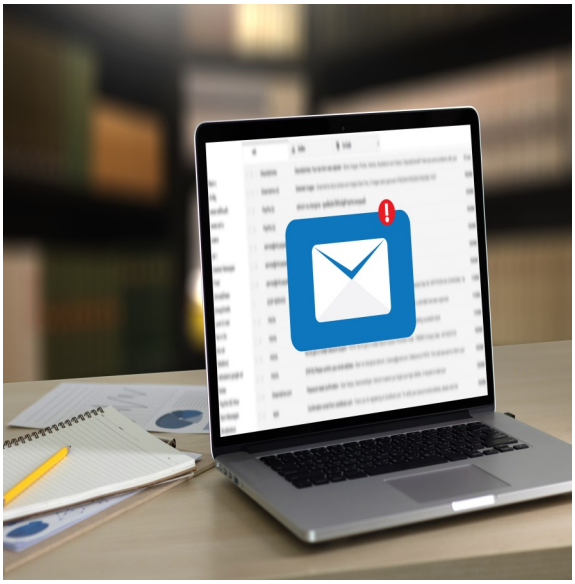
Mobile Banking App is HERE!

UNION BANK

AUGUST 2019 Issue 8

ARE YOU A TARGET?



Many people mistakenly believe they are not a target for cyber attackers: that they, their systems, or accounts do not have any value or that these types of things only happen to big businesses with complicated balance sheets. This could not be further from the truth. If you use technology in anyway, at work or at home, you have value to the bad guys. But, you are in luck. You already have the best defense there is against these cyber attacks - you.

Why You Are a Target

There are lots of different cyber attackers on the Internet today, and they all have different motivations. So why would any of them want to attack you? Because by hacking you they help achieve their goal. Here are two common examples of cyber attackers and why they would target you.

Cyber Criminals: These guys are out to make as much money as possible. What makes the Internet so valuable to them is they can now easily target everyone in the world with just the push of a button. They don't need to match a name to a face all they need to do is access a device. And there are A LOT of ways they can make money from you. Examples include stealing money from your bank or retirement accounts, creating a credit card in your name and sending you the bill, using your computer to hack other people, or hacking your social media or gaming accounts and selling them to other criminals. The list is almost endless and it continues to grow. There is no shortage of ways bad guys can make money off you. There are hundreds of thousands of these bad guys whose sole purpose when they wake up each morning is hacking as many people as possible every single day, including you.

EQUAL HOUSING LENDER Member FDIC

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

Continued on page 2

Targeted Attackers: These are highly trained cyber attackers, often working for governments, criminal syndicates, or competitors targeting you at work. You may feel your job would not attract much attention, but you would be very surprised.

⇒ The information you handle at work has tremendous value to different companies or governments.
⇒ Targeted attackers may target you at work not because they want to hack you, but to use you to hack one of your co-workers or other systems.
⇒ These types of attackers may target you at work because of what other companies you work or partner with.

I Have Anti-Virus, I'm Safe

So conventional wisdom will have one believe "Okay, so I'm a target, not a problem. I'll just install anti-virus and a firewall on my computer and I'm protected, right?" Well unfortunately, no. Many people feel if they install some security tools then they are secure. Of course anti-virus is a great tool to help fight against an attack however, that alone is not enough. Cyber attackers continue to get better and better, and many of their attack methods now easily bypass security technologies. For example, they often create special malware that your antivirus cannot detect. They bypass your email filters with a customized phishing attack or call you on the phone and trick or scam you out of your credit card, money, or password. Technology plays an important role in protecting you, but ultimately you are the best defense.

Fortunately, being secure is not that hard; ultimately common sense and some basic behaviors are your best defense.

- If you get an email, message, or phone call that is extremely urgent, odd, or suspicious, it may be an attack.
- To ensure your computers and devices are secure, keep them current and enable automatic updating.
- Be selective of about what information is shared on social media.
- Finally, use a strong, unique password for each of your accounts.

We all have busy lives and understanding the latest cyber security lingo may not be a top priority. But in the age of technology changing and improving at rapid speed it is imperative for everyone to stay abreast of methods to protect their data on the internet. Being cyber ware is ultimately your best defense.

Source:
Matt Bromiley, Consulting Director,
SANS Ouch! Newsletter, December 2018

PASSWORD SPRAYING:

How to Protect Your Organization From Falling Victim

Cybersecurity professionals are constantly working to try to prevent the next cyberattack or to find a solution if there is one. It's a never ending race against time; no sooner than when a threat is mitigated, a new one emerges to take its place. In this ongoing cycle, passwords have always played a crucial role as the main entry point for cyber criminals, and password spraying is one of the many reasons having a strong password is important.

Password spraying is an attack that attempts to access a large number of account usernames with a few commonly used passwords. Traditional brute-force attacks attempt to gain unauthorized access to a single account by guessing the password. Hackers can use multiple iterations using a number of different passwords, but the number of passwords attempted is usually low when compared to the number of users attempted. This method avoids password lockouts, and it is often more effective at uncovering weak passwords than targeting specific users. During a password-spray attack, cybercriminal uses a single commonly used password for example '12345 or 'Summer2017' against many accounts before moving on to attempt a second password. The goal is to hopefully have a combination of a user name and password word and allow an entry point to a computer, hence the word "spraying". This technique allows the cybercriminal to lay low and undetected by avoiding rapid or frequent account lockouts. Because these types of attacks normally stay below the radar, they are oftentimes hard to detect.

Password spraying attacks have become the favorite technique of cybercriminals and have proven to be an effective way of infiltrating a network. Many organizations are indeed vulnerable to a password spray attack because they either keep weak default passwords (e.g., on routers) or use passwords that can be easily guessed by attackers.

To avoid falling victim to one of these attacks organizations should take the necessary precautions to help protect their network. Below are some steps that can help minimize risk:

- Making sure that two-factor authentication is enabled on accounts will prevent these types of attacks and will make it much more difficult for hackers to make use of stolen credentials.
- Organizations should monitor log information to see the usernames being logged into. If you see that you have users, especially across multiple users, attempting to log into systems on the network that they never have connected to, that could be a really good indication that you have a password spraying or other brute-force or credential misuse type attack that's taking place.
- Making sure appropriate users are logging into appropriate files. For example, if someone from the accounting department suddenly is trying to connect to human resources files, that's a strong indication that something may be wrong. Those types of activities should be monitored regularly and frequently to make sure that it's not happening.
- Make sure your organization has an effective password policy in place.
- Continue to educate your employees on the importance of creating strong passwords. Ensure they adopt good password practices habits.
- Network traffic data is a good way to detect if a hacker has infiltrated your network. Using Active Directory to correlate where users normally connect on the network will help narrow down abnormalities because when a hacker is in the network, they have all of these usernames they're attempting across many devices.

Ensuring your organization implements strong password policy and encourages good password hygiene can help prevent a password spraying attack against your network.

Sources:
https://searchsecurity.techtarget.com/answer/What-is-a-password-spraying-attack-and-how-does-it-workhttps://www.infosecurity-magazine.com/blogs/protect-organization-password/
https://doubleoctopus.com/security-wiki/threats-and-tools/password-spraying/
https://resources.infosecinstitute.com/password-spraying/#gref