UNION BANK

OCTOBER 2019 Issue 10

UNDERSTANDING SOCIAL ENGINEERING

A common misconception most people have about cyber attackers is that they use only highly advanced tools and techniques to hack into people's computers or accounts. This is simply not true. Cyber attackers have learned that often, the easiest way to steal your information, hack your accounts, or infect your systems is by simply tricking you into making a mistake.

What Is social engineering? Social engineering is a psychological attack where an attacker tricks you into doing something you should not do. The concept of social engineering is not new; it has existed for thousands of years. Think of scammers or con artists, it is the very same idea. What makes today's technology so much more effective for cyber attackers is you cannot physically see them; they can easily pretend to be anything or anyone they want and target millions of people around the world, including you. In addition, social engineering attacks can bypass many security technologies.

Most of the time a hacker might look for a software vulnerability. Security professionals will say the weakest link in the security chain is the human element. Social engineering relies heavily on human interaction and often involves manipulating people into breaking normal security procedures, protocols and best practices in order to gain access to systems, networks or physical locations usually for financial gain. There are several ways a hacker can access a computer network, such as baiting, phishing, pretexting and vishing, just to name a few. These methods have been proven to be very successful ways for criminals to manipulate or trick users into giving up privileged information or access within an organization.

If something seems suspicious or does not feel right, it may be an attack. The most common clues of a social engineering attack include:

- *Someone creating a tremendous sense of urgency.* They are attempting to fool you into making a mistake.
- *Someone asking for information they should not have access to* or should already know, such as your account numbers.
- *Someone asking for your password.* No legitimate organization will ever ask you for that.

Continued on page 2

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

- *Someone pressuring you to bypass or ignore security processes or procedures* you are expected to follow at work.
- *Something too good to be true.* For example, you are notified you won the lottery or an iPad, even though you never even entered the lottery.
- *You receive an odd email from a friend or coworker containing wording that does not sound like it is really them.* A cyber attacker may have hacked into their account and is attempting to trick you. To protect yourself, verify such requests by reaching out to your friend using a different communication method, such as in person or over the phone.

The good news is there are several things an organization and individuals can do to protect themselves:

- *Make sure your network's antivirus software is updated on a regular basis.* Having the latest versions of these software applications on your devices will help ensure they're prepared for the most recent security threats.
- *Pay attention to suspicious emails.* Ask yourself if the email or phone call you received makes sense or seems a bit fishy.
- *Set your spam filters to the highest protection.* Check your settings, and set them to high to avoid risky and unwanted messages clogging up your inbox.
- *Don't download files from unknown senders.* Especially if the subject line reads "URGENT".
- *Security awareness training* is always very helpful. If people know what forms social engineering attacks are likely to take or look like, they will be less likely to become victims.

No one is immune to social engineering attacks. It plagues us online and offline. Your best defense against these kinds of attacks is to educate yourself, be vigilant and aware of the risks.

Sources:
https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering
*https://*us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html
SANS Security Awareness OUCH! Newsletter

THE IMPORTANCE OF ENCRYPTION

The term “encryption” is an important word in the digital environment. Encryption is a powerful tool that can be used to protect an organization and its data as well as individuals and their personal information.

A tremendous amount of sensitive information is housed on networks and devices, such as financial data, personal documents, pictures, and emails. If a device is lost or stolen, all of the sensitive information could be accessed by whoever possesses it. In addition, conducting sensitive transactions online, such as banking or shopping, can be monitored by anyone and lead to information being stolen, such as financial accounts or credit card numbers. Encryption protects this information in these situations by helping ensure unauthorized people cannot access or modify that data.

Today, encryption is far more sophisticated and serves a major purpose by passing a secret message from one place to another, ensuring only those authorized to read the message can access it. When information is not encrypted, it is called plain-text. This means anyone can easily read or access it. Encryption converts this information into a non-readable format called cipher-text. Today’s encryption works by using complex mathematical operations and a unique key to convert your information into cipher-text.

Information is vulnerable when it is in transit and when it is at rest. If the data is not encrypted, it can be monitored, modified, and captured online. Keeping data encrypted increases the integrity of such data and ensures only those who are entitled to access that information can. It protects user's identity and privacy and is most successful when uses as an automatic feature. It should be enabled for everything by default and not looked as a tool used on an as-needed basis.

Data is a commodity and can be used for nefarious acts. Safeguarding your data is a no longer an option in the current digital environment; it is a must. Make note, however, that encryption does not totally exempt your data from being infiltrated, but it can serve as another layer of protection along with other security protections.

Despite knowledge of many of the infamous breaches to hit our news cycles over the past several years, many still have not made the transition to encrypt every device.

Having data encrypted can save an organization and individuals not only from potential data breach but also from a financial loss. It is imperative that encryption be viewed as a integral part of overall digital security and used efficiently and effectively to reduce the risk of breaches.

Sources:
https://digitalguardian.com/blog/what-data-encryption
https://searchsecurity.techtarget.com/definition/encryption
https://www.techworld.com/security/what-is-encryption-3659671/
Source: SANS Ouch!