KEEP MY BANK SECURE

CYBERSECURITY QUESTIONS & ANSWERS PRIMER

HOW DO WE PREVENT CYBER ATTACKS?

There are many tactics that are available to prevent and thwart cyber attacks, but a multi-layered (i.e. multi-factor authentication) approach alongside end-user education is probably the simplest and most critical.

IS MY BANK VULNERABLE?

There is always a chance that your bank infrastructure is vulnerable. However, the best way to know for sure is to find and engage a qualified IT services provider to perform an audit and assessment of your infrastructure and protocols for cybersecurity. Only then will you know your degree of vulnerability and the best steps your financial institution can take to lessen your risk.

WHERE DO THESE ATTACKS COME FROM?

The short answer is, from all over the world. However, as has been recently reported by the U.S. government and intelligence community, we're seeing an increasing number come from Russia, Eastern Europe, and China.

HOW FAST DO THESE ATTACKS OCCUR?

Cyber attacks can start with the single click of a button but can take weeks to fully infect a network and steal data before locking you out of access data.

WHAT ABOUT MY REMOTE EMPLOYEES?

Remote access can always be a weak point for security. However, you don't have to limit your remote employees and their productivity to be able to protect them. Education, software, hardware, and protocols can all be enacted to ensure better cybersecurity, even for remote employees.

DO RANSOMS ALWAYS HAVE TO BE PAID?

Depending on the scale, source, and sophistication of the attack and your backup and recovery systems in place at the time of the attack, not necessarily. With the right systems in place, even partially successful attacks and data lockouts can be circumvented.

HOW DO HACKERS GET INTO A SERVER?

Hackers typically gain access via less obvious means first, like a mobile device or a workstation. Email is an easy and popular place for them to gain access since much information is shared between and amongst employees via email. From there, hackers will typically dig around until they find the servers and the credentials necessary to access them. This is why it is good practice to use separate administrative accounts from your email account(s).

HOW DO WE KNOW A HACKER IS SERIOUS?

You will know a hacker is serious by the amount of evidence of the infiltration of your IT infrastructure. For example, if the hacker has encrypted your data and locked you out, then you can assume they are serious.

Another sign of the seriousness of an attack is the hacker's choice of communication. A serious hacker will usually insist on a sophisticated and non-traceable means of communication.

HOW DO WE TRAIN EMPLOYEES FOR THIS?

Monthly end-user training combined with quarterly testing by a qualified IT security provider is a great place to start in order to introduce and educate employees to cybersecurity best practices and protocols.

CAN WE CATCH THESE CRIMINALS?

Unfortunately, most of these criminals are outside of the United States. Without government and international authority intervention, options to bring them to justice are limited. The best defense is to have a proactive plan and approach to cybersecurity.

WHAT OTHER KINDS OF ATTACKS EXIST?

Other than phishing schemes, there are attacks known as brute-force attacks where the hacker simply uses trial and error to guess credentials. There are attacks that shut down websites, such as denial of service attacks, where a web server is flooded with false data requests. There is also a credential stuffing attack, where a hacker gains access to one's password and login credentials and then proceeds to try the credentials across multiple sites and networks. This approach counts on users using the same login credentials for different networks and services. These are just a few, but there are many others.

HOW DO I KNOW IF MY BANK IS A TARGET?

Anyone and everyone can be a target. If you receive spam mail, you have most likely been targeted. If you have received an email that attempts to get you to click on a link by evoking an emergency or urgent situation, you have definitely been a target. Hackers count on volume and the weakest link to gain access to organizational data. This is usually through employees and staff.

WHAT KINDS OF PASSWORDS DO WE SET?

Passphrases should be used instead of passwords. This allows a longer character count while still making it easier for the end-user to remember. And, never use easily guessed content in your passwords or passphrases (e.g. "password", your name, sequential numerals, etc.)

HOW OFTEN DO WE CHANGE PASSWORDS?

You should change passwords at least every 90 days unless you have complex passphrases in place. However, even then, it's wise to periodically change them.

Note: this document is provided by KeepMyBankSecure.com and is intended a public service. It may be copied and distributed internally for use by institutions, except for commercial purposes or republication without the express consent of KeepMyBankSecure.com.