MASTER YOUR CARD

EMPOWERING YOUR COMMUNITY

CYBER READINESS IS CRITICAL FOR BUSINESS OWNERS

A cyberattack affects more than your bottom line; it can affect your organization's reputation as well. In today's connected world, businesses of all sizes may be vulnerable to cyberattacks. Every organization is connected in today's digital world, and cybersecurity is only as strong as its weakest link. 95% of all cyber security incidents involve human error. The FBI reported more than $3.5 billion dollars were lost to Cyber Crime Globally in 2019.

A breach of your organization's cybersecurity can harm your customers, partners and employees. 60% of small companies go out of business within six months of a cyber attack. Understanding these risks and protecting your organization is the first step to becoming cyber ready.

Authentication

Passwords are the gatekeepers to your most important information. Cyber attackers are opportunistic and can easily crack a weak password.

TIPS: Every time you create a password, you should keep the following in mind:

- 8 or more characters
- Uppercase and Lowercase characters
- Use numbers (0 through 9)
- Non-alphanumeric characters
- No words from the dictionary
- No personal inflammation such as date of birth, names, etc.
- Never use the same password on multiple sites
- Change passwords regularly (every three months)
- Don't share passwords

63% of data breaches result from weak or stolen passwords.

90% of employee passwords can be cracked in six hours by hackers.

Over **20%** of business employees have shared their password with assistants or co-workers.

81% of hacking-related breached are the result of either stolen and/or weak passwords.

Phishing

They will try to get you to share sensitive information like passwords, or to click on a link or attachment. This can put malicious software on your computer, putting your identity or organization at risk.

TIPS: Check the sender. Never share sensitive information. If in doubt, don't click. Confirm the sender before clicking on unknown and potentially suspicious links received via text or email.

91% of all cyber attacks start with a phishing email.

89% of phishing attacks mimic corporate emails.

88% of Organizations Reported Experiencing Phishing Attacks in 2019.

76% of organizations reported being the victim of a phishing attack in 2016.

81% of companies that fell for a phishing attack lost customers.

84% of small business are targeted by Phishing Attacks

USBs/Removal Media

USBs and other types of removable media are a handy way to share information. But they are often infected with malicious software that can damage your systems, and there's no way to tell until it's too late. So be USB smart.

TIPS: Always buy your flash drives from reputable manufacturers as well as sellers or consider throwing away your USB drives and move to the cloud for file storage. Never plug unknown flash drives into your computer and don't use the same flash drives for home and work computers.

27% of malware infections for SMBs originated from infected USBs.

87% of employees have lost a USB memory device and not told their employer.

48% of USB sticks found are plugged into a computer within 10 hours of being picked up.

Patching

Patches are regular updates to your software, systems and applications. Updating your devices may be a little annoying, but these critical security updates protect against hackers looking for cracks to slip through.

TIPS: Always update all of your devices as soon as possible.

80% of attacks use computer vulnerabilities for which patches already exist.

In 2019, there were **812.67 million** reported malware infections.

Ransomware

It is a type of malware that prevents or limits users from accessing their systems or devices and demands users pay a ransom by a certain deadline to regain control of their data.

TIPS: Do not pay the ransom. Disconnect your device from the internet or other network connections (such as home Wi-Fi) as soon as possible in order to prevent the infection from spreading. Notify your payment partners. Visit www.nomoreransom.org to check whether your system has been infected with one of the ransomware variants for which there are decryption tools available free of charge.

20% of small business owners report being victims of one or more ransomware attack.

$377,000 is the average ransomware demand.

16.2 days is the average duration a ransomware incident lasts.

At Mastercard, our mission is to de-mystify and simplify cyber readiness. The free Cyber Readiness Program guides you through selecting a Cyber Leader, implementing practical policies and gaining commitment from your workforce. We provide policy templates, training materials, and communication kits developed by leading experts to get your organization cyber ready quickly and efficiently.

To learn more visit: **https://www.mastercard.us/en-us/businesses/small-business/safety-and-security/cyber-security.html**

About Master Your Card:
Master Your Card is a community empowerment education program sponsored by Mastercard, that works with committed partners nationwide to bring information about the benefits of electronic payments technology for underserved communities to build brighter financial futures. The program has facilitated presentations and workshops in numerous cities around the country, provided financial education to tens of thousands of students and reached millions through partners' initiatives and education materials.