Banking locally EVER AFTER IS KEEPING YOUR INFORMATION SAFE

CYBER SECURITY

Times have changed remarkably over the last few years, in both positive and negative ways. One of the more pressing issues is the reality that we can become a victim without seeing an attacker. Global security firm McAfee found in a recent study that despite awareness of the need for cyber security, many are not taking sufficient steps to keep our information protected. An estimated 61% of consumers surveyed claimed that they are more worried about cyber security today than they were five years ago. And, as one high-profile example, the CEO of Equifax attributed the company's 2017 breach—which compromised the data of over 147 million consumers and could cost over $600 million—to human error.

The point is, cyber security threats abound, but there are small things we can each do to stay better protected.

Common Cyber Security Risks

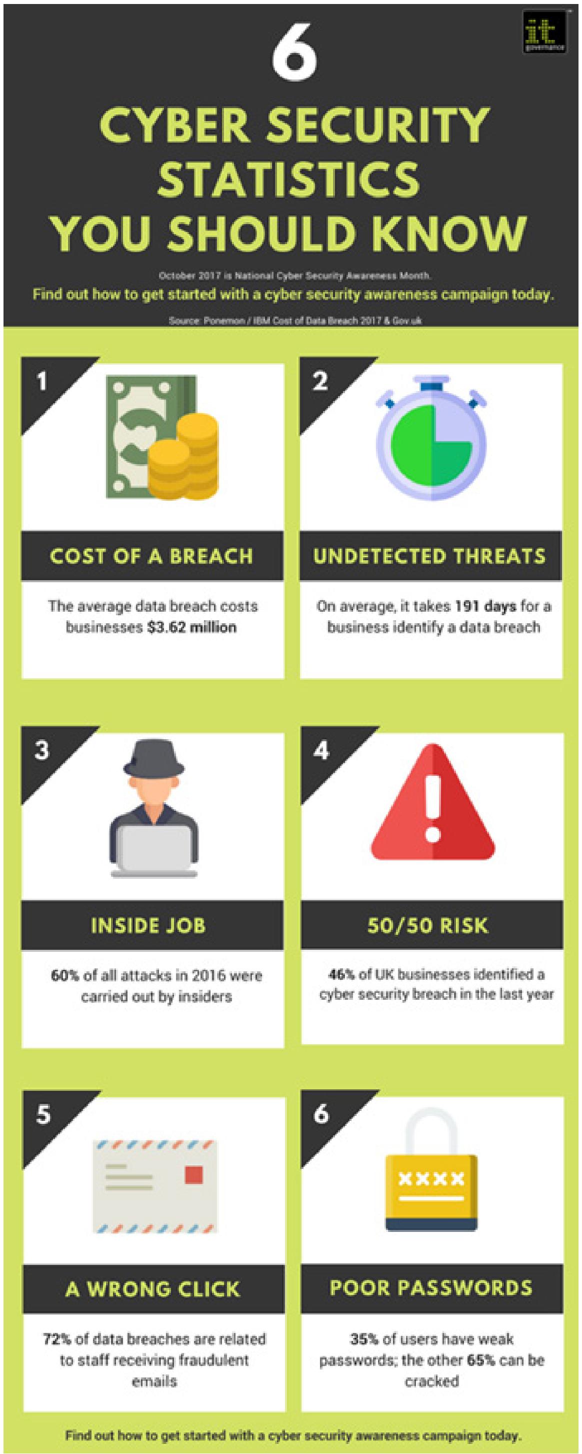
Identity theft (ID theft) occurs when someone assumes another person's personal identifying information (e.g., a name, Social Security number, or date of birth) with the intent of committing fraud. This sensitive information could be used to open new bank or credit accounts, file income tax returns, or apply for government benefits. The impacts can be far-reaching, and in today's ever-connected environment, ID theft is among the largest growing crimes. In fact, new methods of ID theft are turning up constantly.

One example of a newer trend in cyber security is phishing. This type of cyber fraud occurs when a criminal impersonates a real person or organization using email, faxes or websites in an attempt to lure recipients into revealing confidential information. The tone of the communication is often urgent, leading recipients to believe there is something wrong.

Similarly, malware or "malicious software" is an often-seen cyber security risk. Malware is designed to infiltrate a computer system without the owner's knowledge. The term malware encompasses many different types of cyber security threats, including computer viruses, worms, Trojan horses, spyware and other malicious software. Malware for personal smart phones and mobile devices has now entered the market as well, creating even more risk for identity theft.

The Effects of Cyber Security Crimes

The costs of cyber security incidents continue to climb, with the most recent statistics from IBM showing the average cost of a data breach exceeding $3.5 million. While the cyber security industry has been making great strides, cyber criminals are becoming more creative and have diversified their attack strategies. For more than a decade, complex and sophisticated cybercrime organizations focused on large organizations. Today cyber criminals are increasingly attacking small businesses and consumers with greater frequency. That means we all must take steps to safeguard our information.



6 CYBER SECURITY STATISTICS YOU SHOULD KNOW

October 2017 is National Cyber Security Awareness Month.

Find out how to get started with a cyber security awareness campaign today.

Source: Ponemon / IBM Cost of Data Breach 2017 & Gov.uk

1 COST OF A BREACH

The average data breach costs businesses **$3.62 million**

2 UNDETECTED THREATS

On average, it takes **191 days** for a business identify a data breach

3 INSIDE JOB

60% of all attacks in 2016 were carried out by insiders

4 50/50 RISK

46% of UK businesses identified a cyber security breach in the last year

5 A WRONG CLICK

72% of data breaches are related to staff receiving fraudulent emails

6 POOR PASSWORDS

35% of users have weak passwords; the other **65%** can be cracked

Find out how to get started with a cyber security awareness campaign today.

Action Items to Prevent Cyber Security Threats

Preventing ID theft that is the result of cyber security crimes requires some vigilance on behalf of consumers and businesses. The most important steps to take include the following:

- ✓ Install and maintain current anti-virus software on all devices, including mobile phones and tablets.
- ✓ Never click on links or open attachments in emails from unknown senders, and ignore and delete unsolicited requests for personal information.
- ✓ Change default passwords right away and set strong passwords that are difficult to guess or connect back to you.
- ✓ Limit your use of public Wi-Fi, avoiding use for online banking and shopping.
- ✓ When shopping online, look for a padlock symbol next to the browser's address bar and "https://"at the beginning of a web address. This indicates the web site owner has taken steps to assure the page and your information are secure
- ✓ Use discretion about posting personal information on social networking sites. The details can be used to help guess passwords or gather enough information to persuade you to give more personal details.
- ✓ Add email or text message alerts to your accounts. These notifications can help alert you to potentially fraudulent activity and allow you to react more quickly.
- ✓ Use multi-factor authentication (MFA) when available on websites that include personal or payment information.

Top Resources

To learn more about cyber security trends and prevention tactics, use the following expert resources.

8 cyber security trends to watch for 2018*

Survey on Identity Theft, Family Safety and Home Network Security*

*You will be linking to another website not owned or operated by the bank. We are not responsible for the availability or content of this website and do not represent either the linked website or you, should you enter into a transaction. You are encouraged to review the privacy and security policies which may differ from ours.