CyberSecurity
QUICK REFERENCE GUIDE

SOUTH JERSEY TECHIES
MANAGED IT | WEB | CLOUD | VoIP | CABLING | WiFi

SECURITY RISKS

Businesses are at risk for security breaches. Whether a company is thinking of adopting cloud computing or just using email and maintaining a website, cybersecurity should be a part of the plan. Theft of digital information has become the most commonly reported fraud, surpassing physical theft.

Cyber attacks happen every **39 seconds, 95%** are human error

43% of all cyber-attacks are aimed at small businesses

43% of SMBs do not have a cyber security plan in place

Global annual cost of cyber-crime exceeds **$8 trillion**

CONFIDENTIAL INFORMATION

When being trusted with confidential information you must stride towards ensuring this information is never viewed by unauthorized parties. To do so you must ensure your information is confidential, has integrity and is available for when you need it.

Confidential information includes:

Personal Information:

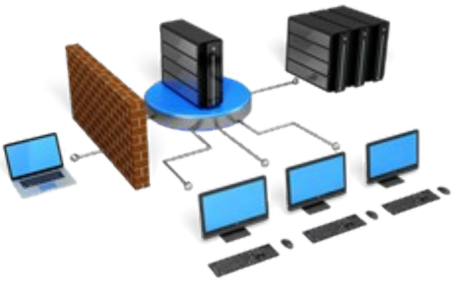
* Social Security Number
* Home Address
* Salary History
* Performance Issues
* Credit Card

Corporate Information:

* Company Unique Processes
* Customer Lists
* Research and Development
* Business Strategies
* Objectives and Projections

FIREWALLS

A firewall acts like a security guard and prevents unauthorized people or programs from accessing a network or computer from the Internet. There are hardware based firewalls, which create a protective barrier between internal networks and the outside world, and software firewalls, which are often part of your operating system.



PASSWORDS

The first line of defense in securing your accounts or computer against unauthorized access is using complex passwords. Complex passwords are exponentially more difficult to crack. Here is a comparison of simple versus complex passwords and how long it would take to crack them.

Character Count	Numbers Only	Upper/Lower Letters	Numbers, Upper/Lower Letters	Numbers, Upper/Lower, Symbols
4	Immediately	Immediately	Immediately	Immediately
6	Immediately	Immediately	1 second	5 seconds
8	Immediately	22 minutes	1 hours	8 hours
10	Immediately	1 month	7 months	5 years
12	25 seconds	300 years	2,000 years	34,000 years
14	45 minutes	800,000 years	9M years	200M years
16	2 days	28N years	37BN years	1TN years
18	9 months	6TN years	100TN years	7QD years

Now that we understand why we should have more complex passwords, here's how we can increase your password's complexity:

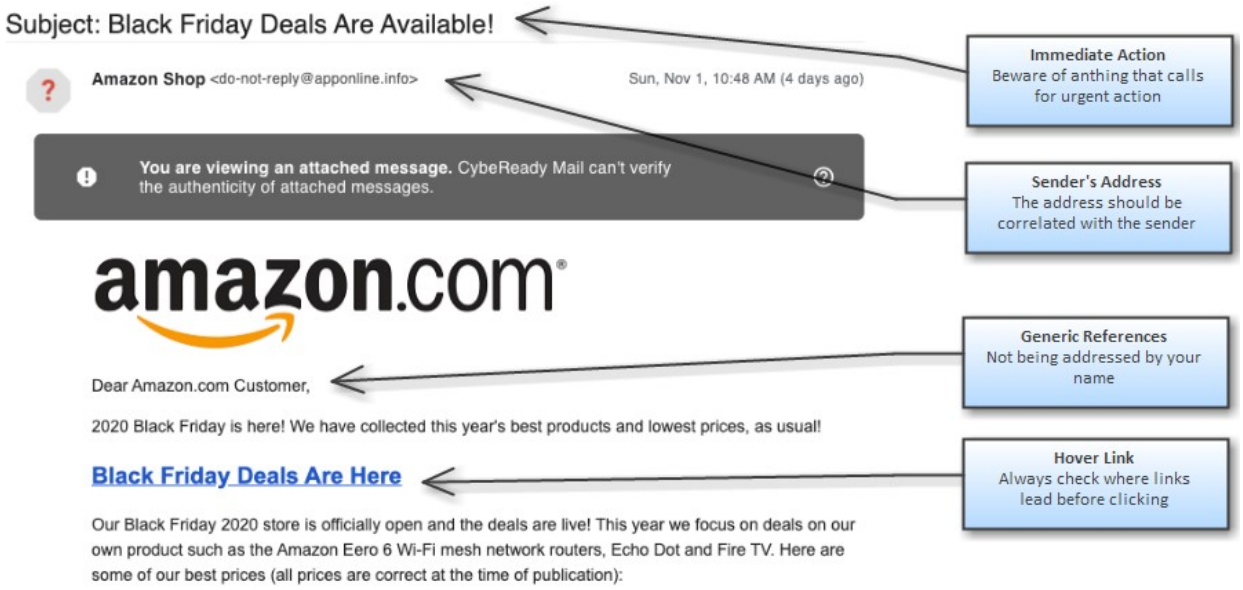
* Bigger is better. Make your password at least 12 characters long, including a combination of numbers, uppercase and lowercase letters, and special characters. This significantly increases the number of possible characters your password could have, thereby increasing the time it would take for a hacker to crack it.
* Avoid using any personal information. Exclude important dates like birthdays, year of graduation, where you went to school, anniversaries, addresses, pet names, and children's names. This information is often available online through publicly accessible sources or social media. If you're a target for hackers, they will use this information to more easily crack your password.
* Do not reuse passwords on multiple accounts.
* Make it easy for you to remember but difficult for others to guess. Consider using a memorable phrase like "4DogsJumpedOver^".

CyberSecurity
QUICK REFERENCE GUIDE

SOUTH JERSEY TECHIES
MANAGED IT | WEB | CLOUD | VoIP | CABLING | WiFi

EMAIL PHISHING and AWARENESS

Phishing has become very sophisticated and difficult to detect, as criminals have found ways to make their emails as realistic as possible. A phishing email tries to trick users into providing confidential data to steal money or information. These emails appear to be from a credible source, such as a bank, government entity, or service provider. Here are some things to look for in a phishing email:



VIRUS & MALWARE PROTECT

If you use a computer for work, web surfing, shopping, banking, email and instant messaging and do not have proper protection, you are at high risk of being victimized. Malware is short for "malicious software." It is written to infect the host computer. Running virus protection products and keeping them up-to-date is and essential step to reduce risks from malware and can reduce infection by more than 80%. Comparing traditional antivirus software with advanced Endpoint Detection and Response solutions, which offer more comprehensive A.I. oriented threat detection and response capabilities

* Keep software/browser/ systems up to date
* Install antivirus software
* Turn on firewall to highest level
* Regularly back up your data
* Do not install or use pirated software
* Do not install P2P file-sharing programs

INTERNET & SOCIAL MEDIA

* Download software only from trusted sources
* Always log out of sites instead of simply closing the window
* Check for https:// in web addresses or secure session validation when available
* Do not click on links from unknown or untrustworthy sources
* Do not allow ecommerce sites to store your credit card information
* Do not click on popup windows to close them; instead use the "X" in the upper right hand corner of the screen
* Call the person who sent the email to confirm its authenticity if you suspect it may be fraudulent
* Limit the amount of personal information you give out
* Use privacy settings online wherever possible
* Do not respond to requests for personal or financial information in an email
* Do not assume that every email you get is authentic (or its attachments)