Security Basics

Quick Reference Guide

Security Risks

Businesses worldwide are at risk for security breaches. While large, well-known companies seem like a likely target, small and medium-sized organizations and individuals are also at risk. There are many ways data can be compromised, including viruses, phishing scams, hardware and software vulnerabilities, and network security holes.

Did you know?

11% of U.S. adults have had personal information stolen

1 in 5 people have had an email or social media account hacked

98% of software applications are vulnerable

Only **40%** of adults know how to protect themselves online

Confidential Information

When dealing with security, confidentiality means private information is never viewed by unauthorized parties. Confidential information must only be accessible to those authorized to view the sensitive data. Confidential information includes:

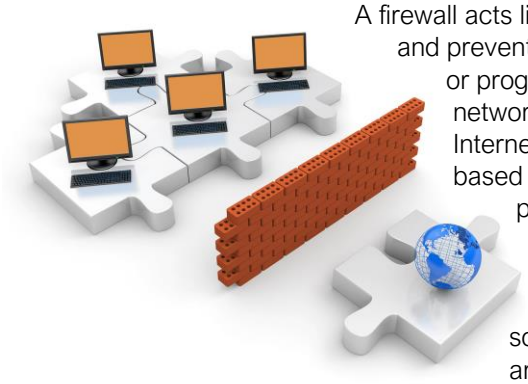
Personal Information

- Social Security Number
- Home Address
- Salary History
- Performance Issues
- Credit Card Numbers

Corporate Information

- 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 maintaining system security is using complex passwords. Use passwords that are at least 8 characters long and include a combination of numbers, upper and lowercase letters, and special characters. Hackers have tools that can break easy passwords in just a few minutes.

How Long Does it Take to Crack a Password?

There are 2 kinds of passwords:

Simple

Lowercase letters only

Complex

Upper & lowercase letters, numbers, & special characters

Complex passwords are **EXPONENTIALLY** More difficult to crack

Use them!

Here's how long it takes to crack a password when it's **simple** vs. **complex**

Characters	Password	Time to crack
8	ghiouhel	4 hours, 7 min
	ghiouH3l	6 months
9	houtheouh	4 days, 11 hours
	Houtheo!2	1060 years
10	ghotuhilhg	112 days
	gh34uhilh!	1500 years
11	wopthiendhf	8 years, 3 months
	w3pthi7ndh!	232,800 years
12	whithgildnzq	210 years
	@hi3hg5ldnq!	15,368,300 years

Source: mywot.com

Malware

Malware is short for "malicious software." It is written to infect the host computer. Common types of malware include:

VIRUS

Replicating computer program that infects computers

ADWARE

Hijacks your computer or browser and displays annoying advertisements

SPYWARE

Secretly tracks your internet activities and information

TROJAN

Malicious program that tries to trick you into running it

Online Browsing

Browsers communicate to websites with a protocol called HTTP, which stands for Hyper Text Transfer Protocol. HTTPS is the secure version of HTTP. Websites that use HTTPS encrypt all communication between your browser and the site.

Secure sites have an indicator, like a padlock, in the address bar to show the site is secure. You should always ensure security when logging in or transferring confidential information.

Sites without HTTPS are not secure and should never be used when dealing with personal data. If you are simply reading an article or checking the weather, HTTP is acceptable.

Network Security

- Use Wi-Fi password security and change the default password
- Set permissions for shared files
- Only connect to known, secure public Wi-Fi and ensure HTTPS-enabled sites are used for sensitive data
- Keep your operating system updated
- Perform regular security checks
- Browse smart!

Email and Phishing

A phishing email tries to trick consumers 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:

Grammatical Errors

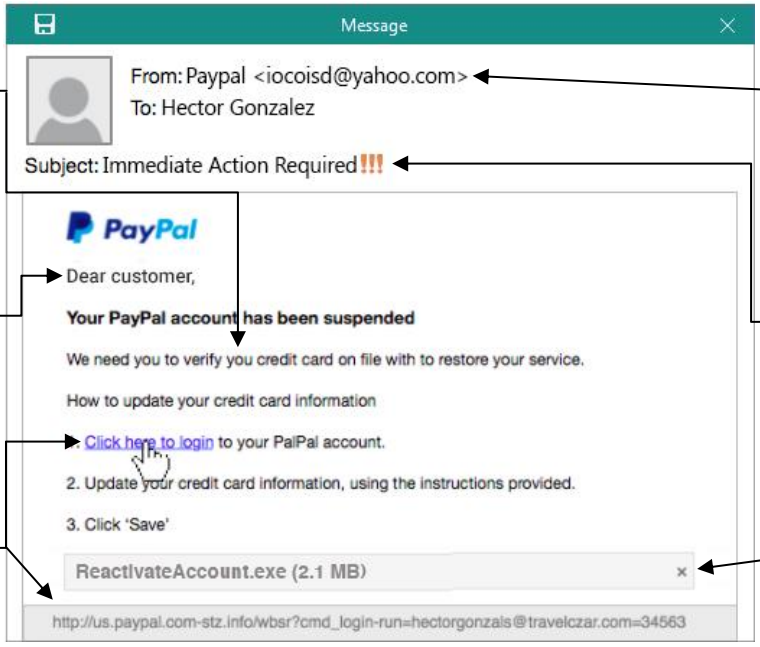
Spelling mistakes and poor grammar

Generic References

Not being addressed by your name

Hover Link

Always check where links lead before clicking



Sender's Address

The address should be correlated with the sender

Immediate Action

Beware of anything that calls for urgent action

Attachments

Never open an attachment you aren't expecting