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

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

<table>
<thead>
<tr>
<th>Characters</th>
<th>Password</th>
<th>Time to crack</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>ghiouhel ghiouH3!</td>
<td>4 hours, 7 min 6 months</td>
</tr>
<tr>
<td>9</td>
<td>houtheouh Houtheo!2</td>
<td>4 days, 11 hours 1060 years</td>
</tr>
<tr>
<td>10</td>
<td>ghotuhilihg gh34uhihl!</td>
<td>112 days 1500 years</td>
</tr>
<tr>
<td>11</td>
<td>wopthiendhf w3ph7i7ndh!</td>
<td>8 years, 3 months 232,800 years</td>
</tr>
<tr>
<td>12</td>
<td>whithgildnzq @hi3h5gldnq!</td>
<td>210 years 15,368,300 years</td>
</tr>
</tbody>
</table>

Source: mywot.com

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.
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.

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
- **Immediate Action**: Beware of anything that calls for urgent action
- **Attachments**: Never open an attachment you aren’t expecting

**Message**

From: Paypal <ielcoost@yahoo.com>
To: Hector Gonzalez
Subject: Immediate Action Required!!!

Dear customer,

Your PayPal account has been suspended.
We need you to verify your credit card on file to restore your service.
How to update your credit card information:

1. Click here to login to your PayPal account.
2. Update your credit card information, using the instructions provided.
3. Click ‘Save’.

ReactivateAccount.exe (2.1 MB)

http://us.paypal.com/statinfo/bsr?cmd_login-run=hectorgonzales@travelzar.com@48583

**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

Loved by Learners, Trusted by Trainers
Please consider our other training products!

Interactive eLearning
Get hands-on training with bite-sized tutorials that recreate the experience of using actual software. SCORM-compatible lessons.

Customizable Courseware
Why write training materials when we've done it for you? Training manuals with unlimited printing rights!

Over 3,000 Organizations Rely on CustomGuide

The toughest part [in training] is creating the material, which CustomGuide has done for us. Employees have found the courses easy to follow and, most importantly, they were able to use what they learned immediately.