CYBERSECURITY

Your Guide to Online Safety and Security

Protect your organization by creating
a safe cyber environment.

GUIDEONE™
INSURANCE

You provide a great service to your community.

And to keep your building, assets and community members safe, you install various security measures.

It's important to do the same for your intangible asset — the information and data you keep stored online, such as your members' personal and financial information or your organization's funds and donations.

Our risk management experts at GuideOne Insurance created this cybersecurity guide to help you stay safe online.

DOS AND DON'TS

Do:

+ Change your passwords often and increase their strength by adding numbers and symbols.
+ Regularly update your operating system and be sure to use licensed anti-virus software. Be wary of pop-up and free ads on the Internet.
+ Log out of all electronic devices when you're done using them.
+ Check websites for a secure URL that includes https://. A URL without the "s" (http://) is unsecure.
+ Be wary of your privacy settings and the content you post on social media. Set all accounts to private and never post sensitive information or click on strange links.
+ Alert the appropriate system administrators if you believe you may have been compromised and change all passwords.

Don't:

+ Store your passwords in an easily accessible place, like a sticky note on your desk.
+ Use common passwords such as:
  - 1234567
  - Password
  - Incorrect
  - 11111
  - abc123
  - Birthdate
+ Leave any device logged in and unattended for even a short period of time.
+ Open emails or attachments from unknown sources or plug in unknown flash drives, external hard drives or smartphones.
+ Conduct online transactions, like banking or shopping, while connected to public Wi-Fi.
+ Store your card details on websites.
+ Remain quiet or feel ashamed if your information has been compromised. Even the most tech-savvy people have been hacked. If you've been hacked, time is the ultimate enemy.

GLOSSARY

Adware

Unwanted pop-up ads that keep tabs on your browsing activity. Adware is often annoying and occasionally malicious.

Anti-Spyware Software

A program that specializes in detecting and blocking, or removing, forms of spyware (definition under Malware). Most anti-virus or anti-malware software includes a level of anti-spyware protection. A single product that covers both would be beneficial to your organization.

Anti-Virus Software

A program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents.

(This is sometimes achieved by removing or neutralizing the malicious code.)

Cybersecurity

The overall protection of computer systems against damage, exploitation, modification and unauthorized use.

Data Breach

The unauthorized release of sensitive information to a party (usually outside the organization) that is not authorized to have or see the information.

Digital Signature

A mathematical technique that is used to validate the authenticity and integrity of a message, software or digital document.

Firewall

A network security system that watches network activity and helps keep the bad stuff (hackers, malware, etc.) out. It's like a first line of defense for your computer.

Malware

Malicious software or code that typically damages or disables, takes control of or steals information from your computer system. Forms of malware include viruses, spyware, Trojan horses, worms, backdoors, boot kits, logic bombs and rootkits.

+ **Rootkits** – Malware that provides privileged (root-level) access to your computer.
+ **Spyware** – Software that is secretly installed into an information system, without your knowledge, in order to gather information about you.
+ **Virus** – A program that spreads by first infesting files or the system of a computer or network router's hard drive and then making copies of itself. Viruses are primarily shared through email and require some sort of user action to spread (i.e., opening an attachment, visiting a malicious website).
+ **Worm** – A type of virus that self-replicates within a network or system, meaning it can spread from computer to computer without human interaction. It hogs memory and network bandwidth, which can cause your computer to stop responding.

Patch

An update to a vulnerable program or system. A common practice to keep your computer and mobile devices secure is installing the vendor's latest patches in a timely fashion. Some vendors release patches on a monthly or quarterly basis. Therefore, having a computer that is unpatched for even a few weeks could leave it vulnerable.

Phishing

The most common form of social engineering in which a malicious entity sends an email from what appears to be a trusted source. They might look like they come from your bank, your child's school or a friend, and they may even create a very similar-looking website. Often, attackers take advantage of current events or times of the year such as: natural disasters, epidemics and health scares, major political elections and holidays.

There are indicators you can look for to judge whether an email is real or a phishing scam. Scams usually use an insecure website (http), come from a personal email (Gmail, Yahoo, etc., versus a company site) and/or create urgency and portray a sense of danger (i.e., we will close your account in five days if you do not respond).

Social Engineering

Most cyberattacks fall under a category called "social engineering" in which third parties get access to vital information and systems through thoughtful planning and execution. Essentially, they work as con artists to entice you into clicking a link and/or entering personal information by pretending to be someone you know or trust, such as your bank or even your friend.

Spoofing

Forgery of an email header in which the message appears to have originated from someone or somewhere (usually a trusted source) other than the actual source.

Trojan Horse

A computer program that is hiding a virus or other potentially damaging program. It may come from software downloaded for free from an attachment in email messages.

How can we help you and your organization in your mission to make a difference? Call us today to find an agent or get a free, no-pressure quote and insurance proposal. **1.888.218.8561**

1111 Ashworth Rd / West Des Moines, IA 50265 / 1.888.218.8561 / **GuideOne.com** /

Sources: US-CERT/TechTarget/EiQ/NICCS/UMUC

CM 18126 (04/18)