Risk Control Technical Bulletin

October 4, 2021

Statewide Insurance Fund

CYBERSECURITY AWARENESS MONTH - WEEK 1 #BECYBERSMART

The first week of Cybersecurity Awareness Month we will explore cybersecurity fundamentals. Owning your role in cybersecurity and starting with the basics in protecting our information is the first line of defense we can take to enhance our cybersecurity without requiring a significant investment or the help of security professionals.

The National Cybersecurity Alliance has highlighted eight basics steps that we can put into action now to reduce our cyber risks. The Fund strongly recommends our members to follow the following steps.

Step 1: MAKE A LONG, UNIQUE PASSPHRASE Length trumps complexity. A strong passphrase is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember.

Step 2: PASSPHRASES AREN'T ENOUGH Use 2-factor authentication or multi-factor authentication (like biometrics, security keys or a unique, one-time code through an app on your mobile device) whenever offered.

Sept 3: WHEN IN DOUBT, THROW IT OUT Links in email, tweets, texts, posts, social media messages and online advertising are the easiest way for cyber criminals to get your sensitive information. Be wary of clicking on links. Essentially, just don't trust links.

Step 4: KEEP A CLEAN MACHINE Keep all software on internet connected devices – including personal computers, smartphones and tablets – current to reduce risk of infection from ransomware and malware. Configure your devices to automatically update or to notify you when an update is available.

Step 5: BACK IT UP Protect your valuable work, photos and other digital information by making an electronic copy and storing it safely. If you have a copy of your data and your device falls victim to ransomware or other cyber threats, you will be able to restore the data from a backup.

Step 6: OWN YOUR ONLINE PRESENCE Every time you sign up for a new account, download a new app, or get a new device, immediately configure the privacy and security settings to your comfort level for information sharing. Regularly check these settings (at least once a year) to make sure they are still configured to your comfort.

Step 7: SHARE WITH CARE Think before posting about yourself and others online. Consider what a post reveals, who might see it and how it might affect you or others.

Step 8: GET SAVVY ABOUT WIFI HOTSPOTS Public wireless networks and hotspots are not secure, which means that anyone could potentially see what you are doing on your laptop or smartphone while you are connected to them. Limit what you do on public WiFi, and avoid logging in to key accounts like email and financial services. Consider using a virtual private network (VPN) or a personal/mobile hotspot if you need a more secure connection.

Statewide Insurance Fund

One Sylvan Way Suite 100
Parsippany, NJ 07054

Phone: 862-260-2050
Email: bruch@sifnj.com

NATIONAL CYBERSECURITY ALLIANCE

OWN YOUR ROLE IN CYBERSECURITY: START WITH THE BASICS

Every individual should **own their role** in protecting their information and securing their systems and devices. There are many steps individuals can take to enhance their cybersecurity without requiring a significant investment or the help of an information security professional.
Below, NCSA highlights eight tips you can put into action now:

CYBERSECURITY BASICS:

MAKE A LONG, UNIQUE PASSPHRASE

Length trumps complexity. A strong passphrase is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember.

PASSPHRASES AREN'T ENOUGH

Use 2-factor authentication or multi-factor authentication (like biometrics, security keys or a unique, one-time code through an app on your mobile device) whenever offered.

WHEN IN DOUBT, THROW IT OUT

Links in email, tweets, texts, posts, social media messages and online advertising are the easiest way for cyber criminals to get your sensitive information. Be wary of clicking on links or downloading anything that comes from a stranger or that you were not expecting. Essentially, just don't trust links.

DEFINITION OF CYBERSECURITY:

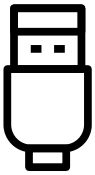
Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack (Merriam-Webster)

KEEP A CLEAN MACHINE

Keep all software on internet connected devices – including personal computers, smartphones and tablets – current to reduce risk of infection from ransomware and malware. Configure your devices to automatically update or to notify you when an update is available.

NATIONAL CYBERSECURITY ALLIANCE

OWN YOUR ROLE IN CYBERSECURITY: START WITH THE BASICS



BACK IT UP

Protect your valuable work, music, photos and other digital information by making an electronic copy and storing it safely. If you have a copy of your data and your device falls victim to ransomware or other cyber threats, you will be able to restore the data from a backup. Use the 3-2-1 rule as a guide to backing up your data. The rule is: keep at least three (3) copies of your data, and store two (2) backup copies on different storage media, with one (1) of them located offsite.

OWN YOUR ONLINE PRESENCE

Every time you sign up for a new account, download a new app, or get a new device, immediately configure the privacy and security settings to your comfort level for information sharing. Regularly check these settings (at least once a year) to make sure they are still configured to your comfort.

SHARE WITH CARE

Think before posting about yourself and others online. Consider what a post reveals, who might see it and how it might affect you or others. Consider creating an alternate persona that you use for online profiles to limit how much of your own personal information you share.

GET SAVVY ABOUT WIFI HOTSPOTS

Public wireless networks and hotspots are not secure, which means that anyone could potentially see what you are doing on your laptop or smartphone while you are connected to them. Limit what you do on public WiFi, and avoid logging in to key accounts like email and financial services. Consider using a virtual private network (VPN) or a personal/mobile hotspot if you need a more secure connection.

ADDITIONAL RESOURCES

- **Cybersecurity & Infrastructure Security Agency:** Cybersecurity Tips
  https://www.us-cert.gov/ncas/tips
- **Cybersecurity & Infrastructure Security Agency:** Protecting Your Privacy
  https://www.us-cert.gov/ncas/tips/ST04-013
- **Federal Trade Commission:** Cybersecurity Basics
  https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/basics
- **Adobe & NCSA Security Awareness Video:** Phishing and Ransomware
  https://youtu.be/D_yAYhjNE-0