CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
CENTER FOR CONSUMER INFORMATION
& INSURANCE OVERSIGHT

# Best Practices for Cybersecurity

According to a Small Business Administration (SBA) survey, 88% of small business owners felt their business was vulnerable to a cyber-attack. Yet many businesses don't know where to begin when it comes to cybersecurity. This tip sheet provides best practices for cybersecurity to agents and brokers to prevent cyber-attacks.

## How to Create a Strong Password

Agents and brokers should use the following tips to create strong passwords that make it more challenging for hackers to gain unauthorized access to their accounts. To maintain good password hygiene, agents and brokers should:

- Make their passwords unique and use a different password for each of their accounts.
- Use passwords that are 8 to 12 characters long.
  - Avoid passwords that could be easily guessed by people they know or by looking at easily accessible information (such as a social media account).
  - An example of a strong password would be "Y&%145zL".
  - An example of a weak password would be "ACAagent91".
- Avoid passwords that contain personal information or common words or phrases. Personal information can include nicknames, birthdays, the name of their street, or the names of family members.
- Review cycle frequency and change their password on a frequent basis to make it more difficult for hackers to track.
- Use Multi-Factor Authentication (MFA) whenever possible to make it more challenging for hackers to gain unauthorized access to accounts.

## How to Use Wi-Fi Safely

Agents and brokers should not use free Wi-Fi networks when accessing accounts with consumer personally identifiable information (PII).

- Hackers can lurk on free Wi-Fi networks such as those at coffee shops, airports, and hotels. Agents and brokers should exercise caution using Wi-Fi when traveling or working remotely. It's recommended to use password-protected Wi-Fi networks only.

> **Scenario:** Taylor is traveling and the hotel she is staying at offers free Wi-Fi. Is it okay for her to use this Wi-Fi to access her business email and protected business files?
>
> **Answer:** No. Connecting to free, unsecure Wi-Fi networks can expose her computer to unnecessary security risks. If she needs to access or send sensitive information while using public Wi-Fi networks, she should use a Virtual Private Network (VPN) service. She can also use her mobile device to create a personal Wi-Fi hotspot that only she, or anyone she grants access, can use.

*If you have any questions or concerns, please contact the Agent/Broker Email Help Desk at FFMProducer-AssisterHelpDesk@cms.hhs.gov*

Updated: August 2022

## How to Use a Virtual Private Network (VPN)

Agents and brokers who need to access public Wi-Fi networks often should consider using a VPN service.

- A VPN service allows you to remotely connect to a corporate network via a secure tunnel. Users can take advantage of the internal services and protections normally offered to on-site users, such as email, sensitive document repositories, and perimeter firewalls.
- Agents and brokers should harden the VPN against compromise by reducing the VPN server's attack surface through:
  - Configuring strong cryptography and authentication
  - Running only strictly necessary features
  - Protecting and monitoring access to and from the VPN

To learn more about VPN networks, see the National Security Administration (NSA) and Cybersecurity and Infrastructure Security Agency's (CISA) information sheet on Selecting and Hardening Remote Access VPN Solutions.

## How to Use Encryption

Encryption is the best tool available to ensure that PII cannot be intercepted. Encryption utilizes a key code, which looks like a random series of letters, numbers, and characters to send sensitive information. Agents and brokers should use encryption when sending documents or emails with consumer PII or other sensitive information. For a step-by-step guide on how to implement encryption see the CISA's tips on Understanding Encryption.

> **Scenario:** Michael needs to send a file with consumer PII to his colleague. How should Michael send this information to his colleague?
>
> **Answer:** First, he should encrypt the file and securely send his colleague the key code. Then, he can send the encrypted file to his colleague via email and his colleague can use the key code to securely access the file.

To learn more best practices for cybersecurity, see this Computer-Based Training (CBT) on the Marketplace and Cybersecurity.