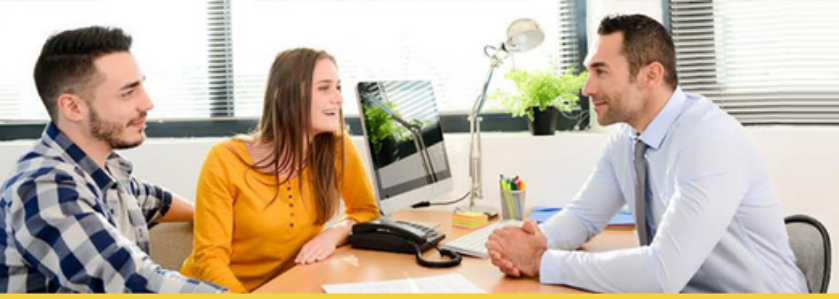


CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
CENTER FOR CONSUMER INFORMATION & INSURANCE OVERSIGHT

Best Practices for Cybersecurity: *Phishing*

As it becomes more common for consumer interactions to occur digitally, it is important that agents and brokers recognize cybersecurity threats and aim to prevent them. Pursuant to 45 CFR § 155.260, the Individual Marketplace Privacy and Security Agreement and SHOP Privacy and Security Agreement, agents and brokers are required to protect consumers' personally identifiable information (PII). Educating consumers about the following phishing best practices is one of the ways agents and brokers can protect consumer PII and threats to their own book of business.

What is Phishing?

Phishing is a form of social engineering whereby intruders seek to gain access to information and information systems by posing as a real person, business, or organization with legitimate reason to request the information. These emails often look real and appear to contain real organizational logos and trademarks. They may be personally addressed to you and appear to be sent from a legitimate source you know and trust, like a government agency or professional organization. Phishing emails (or texts) often alert the user to a problem with their account and ask the user to click on a link to provide information to correct the problem.

How to Recognize Phishing

Agents and brokers should look for potential phishing threats, including urgent messages that:

- Ask them to click on a link to make a payment.
- Say they are eligible for a government refund or free plan.
- Instruct them to provide or confirm personal information.
- Notify them of an issue with their personal information or account.

Other signs of phishing attempts include:

- Poor grammar, typos, and inconsistent formatting.
- A similar, but not identical, sender email address (e.g., “Amazons.com”).
- Suspicious attachments and hyperlinks.
- The use of logos, signatures, or other recognizable features of a company or organization.
- The sender's email address is not recognizable or in your contacts.

How to Avoid Phishing

Agents and brokers can protect themselves from phishing by:

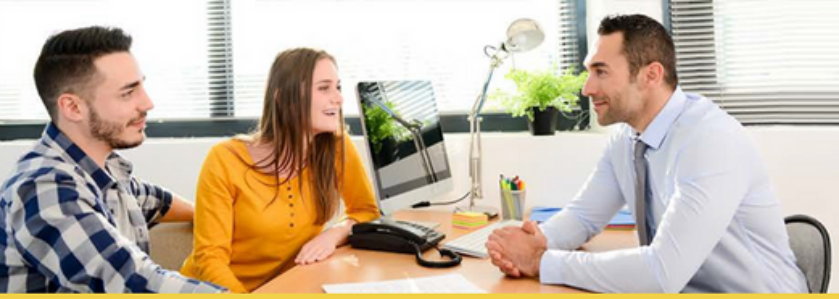
- Maintaining current anti-virus software.
- Regularly updating the software on your computer and cell phone.
- Utilizing a multi-factor authentication (MFA) with all your accounts.
- Backing up the data on your computer and cell phone.
- Filtering spam emails.
- Not clicking links or opening attachments.

For more information on avoiding phishing attacks, see these resources:

- How to Recognize and Avoid Phishing Scams (FTC)
- Avoiding Social Engineering and Phishing Attacks (CISA)

This communication was printed, published, or produced and disseminated at U.S. taxpayer expense. If you have any questions or concerns, please contact the Agent/Broker Email Help Desk at FFMProducer-AssisterHelpDesk@cms.hhs.gov.

Updated: June 2023



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

How to Report Phishing

If you become aware of a breach or incident involving PII as a result of phishing, report this situation immediately to the appropriate organization.

This webpage provides helpful resources for reporting Marketplace fraud.

In addition, change the password to any account that may be compromised.

You can also report the cyberattack to the police, file a report with the Federal Trade Commission, or report the cyberattack to the Federal Bureau of Investigation (FBI), the lead federal agency for investigating cyberattacks and intrusions.

If you or your client believe you are a victim of phishing, do not respond to the suspicious email, text message, or phone call. Instead, contact the individual or organization that is being imitated with the attempt. It's also a good idea to contact your organization's IT department to inform them of the attempt and deter potential attempts in the future.

This communication was printed, published, or produced and disseminated at U.S. taxpayer expense. If you have any questions or concerns, please contact the Agent/Broker Email Help Desk at FFMProducer-AssisterHelpDesk@cms.hhs.gov.

Updated: June 2023