Cyber Security Compliance Training

Heritage Provider Network
&
Affiliated Medical Groups

Table of Contents

At the end of this training, please complete the quiz successfully to receive the “Certificate of Completion”. The training is not complete until the certificate and quiz results are submitted to contact information listed on the certificate.

What is Cyber Safety?

- Cyber Safety is the safe and responsible use of information and communication technology. It is about keeping information safe and secure, but also about being responsible with that information, being respectful of other people online, and using good 'netiquette' (internet etiquette)

- PS: This training material is intended for employees using **company issued workstations, laptops and other devices.**

Cyber Safety Threats

- Viruses: Viruses infect computers through email attachments and file sharing. They delete files, steal or corrupt data, attack other computers, and make your computer run slowly. One infected computer can cause problems for all computers in the same network.

Do’s: Always exercise caution before opening files. Please make sure the file/attachment came from a trustworthy source. Always consult your IT support team when you receive a suspicious email.

Don'ts: Do not open files attached in an email from unknown sources. Don’t download programs/executables from untrusty websites and from external media.

Cyber Safety Threats - Continued

- Hackers: These are people who “trespass” into your computer from a remote location. They may use your computer to send spam or viruses, host a website, or do other activities that cause major computer malfunctions and service disruptions.

Do’s: When you see suspicious files or data loss from your computer, unplug your network cable from the back of your device (or disconnect WIFI) and contact IT support immediately.

Cyber Safety Threats - Continued

Spyware:

- Spyware is software that “piggybacks” on programs you download, gathers information about your online habits, and transmits personal information without your knowledge.
- It is also created with the intent of damaging/disabling computers and computer systems, steal data, or gain unauthorized access to networks.
- It may get installed on a computer when a user clicks on an unsafe link, opens an infected file, OR visits a seemingly legitimate website that could contain malicious software that gets automatically downloaded to your computer.

Cyber Safety Threats - Continued

Spyware:

Do’s: Visit only trustworthy websites that are required to perform your job. Consult IT support before installing any programs or applications. Ensure that you are on a legitimate website before you enter critical and secure member information.

Don'ts: Do not install programs without consent of and consultation by the IT support team.

Cyber Safety Threats - Continued

Phishing:

- Hackers pretend to be a trustworthy source in order to acquire sensitive personal information such as usernames, passwords, social security numbers, and credit card details. An email, phone call or text message from a seemingly legitimate email address or number instructs you to click on a link to take action (e.g., "Validate your account," "Confirm your identity," "Access your tax refund"). The link brings you to a website requiring you to enter your personal information.
- Because the cybercriminal masquerades as a legitimate source (e.g., financial institution employee, client, customer, realtor, banker), you believe the request is from a trusted source and you unwittingly oblige when they ask you for your personal information.
- 70% of cyberattacks use a combination of phishing and hacking.

Cyber Safety Threats - Continued

Phishing:

Do’s: Inform IT support immediately if you see an email with suspicious links embedded in it as there is a good chance others in the organization may have received it as well.

Don'ts: Do not use work email to register for external services like banking, mortgage, taxes, bill pay etc. Do not click on phishing links embedded in the email body.

Cyber Safety Threats - Continued

Credential Replay:

- Many people re-use passwords and usernames (aka ‘credentials’).
- Cybercriminals obtain these login credentials, test them in large numbers against numerous websites to find matches, and then request fraudulent transactions.
- They may resell this information to other cybercriminals to make a profit. This information may then be used to commit fraud.

Do’s: Use separate passwords for all online accounts. Keep changing them at least once every 6 months.

Don'ts: Don’t store your passwords in plain text in your email drafts, file system or online storage media.

Consequences of Inaction

- Loss of access to network
- Loss of confidentiality, integrity and/or availability of valuable patient information
- Lawsuits, loss of public trust, prosecution, internal disciplinary action or termination of employment
- Spyware deletes files or directory information, or it may allow attackers to covertly gather personal data, including financial information and usernames/passwords
- Victims of phishing may have spyware installed on their computer systems or have their identity stolen

Cyber Safety Actions

- The following slides describe the top actions you can take to protect personal information and your computer. These actions will help you meet the HPN Cyber-safety Program policy standards.

- By implementing all of these security measures, you will protect yourself, others, your computer and your network from many common threats.

- In most cases, implementing each of these security measures will only take a few minutes.

Cyber Safety Actions - Continued

Responsible Email Actions:

- Do not click on suspicious links embedded in emails. Hover over questionable links to reveal the true destination before clicking.
- Don’t open attachments or click on URLs in unsolicited emails, even from users you know.
- Alert IT support immediately upon receiving suspicious emails.
- Do not act on email-based requests for sensitive personal information, money movements, or trading. Directly verify all requests with the clients and ask questions.

Cyber Safety Actions - Continued

Responsible Email Actions - Continued:

When an email is received, check the following:

- The email is from a known sender and/or sender in your contacts.
- The email has a proper subject line without spelling errors.
- The email has some content in the body with proper grammar and spelling.
- The content is properly formatted and has a proper signature which includes the sender details.

Cyber Safety Actions - Continued

Responsible Browsing:

- Do not visit websites that are not intended for work.
- Do not download/install/open programs/executables without consulting/reviewing with IT support.
- Beware of cloned websites that may appear to be legitimate. Note that secure websites start with **https**, not http
- Beware of suspicious websites, even if they are https://. Here is an example.

  https://www.bankofamerica.com and https://www.bankofarnerica.com are two different sites, one of them is trying to steal your identity. (Please note how cleverly 'm' was replaced by 'rn')

Cyber Safety Actions - Continued

Responsible use of external media:

- Do not insert any USB drive or CDs/DVDs that you've received from an unknown/unreliable source.
- Do not install programs that was copied from a USB drive, external drive and/or found over the internet.

Cyber Safety Actions - Continued

Software updates and patches:

- Updates - sometimes called patches - fix problems and glitches with your operating system (OS) (e.g., Windows) and software programs (e.g., Microsoft Office applications). Anti-virus software removes viruses, quarantines and repairs infected files, and can help prevent future viruses.
- Please ensure all software patches are installed and kept up-to-date by your IT department.
- To avoid computer problems caused by viruses, please ensure that an anti-virus program like Sophos is installed and kept up to date.

Cyber Safety Actions – Password Protection

- Do not share your passwords at any cause. They **must not** be shared with colleagues, vendors and IT support.
- Change your passwords periodically, at least every 6 months.
- When choosing a password:
  - Mix upper and lower case letters
  - Use a minimum of 8 characters
  - Use mnemonics to help you remember a difficult password
  - Make new passwords difficult to guess by avoiding dictionary words, and mixing letters, numbers and punctuation. Use a unique long and strong password for each account to prevent a quick and invasive attack on all of your accounts. Do not use one of these common passwords or any variation of them: qwerty1, abc123, letmein, password1, iloveyou1, (yourname1), baseball1.

Cyber Safety Basics –Quiz

1. True or False? Viruses can be transmitted via email, email attachments or IM (Instant Messaging).
   __True.
   __False.
2. People who seek out your personal information and then use it to commit crimes are called:_____
   2. Solicitors
   3. Telemarketers
   4. Identity Thieves
   5. Crime busters
3. Which of the following is a way to help prevent identity theft. (Check all that apply.)
   __A. Never send personal information via email or instant messages unencrypted.
   __B. Always send personal information via email or instant messages.
   __C. All of the above
   __D. Don't tell anybody my name.
4. True or False? *Iloveyou2* is a good password. Why or why not?
   __False. Even though it follows all password creation rules, it is a very common password
   __True. The password contains a number, a capital letter, and a lower case letter.

Cyber Safety Basics –Quiz

5. Whose responsibility is it to install Antivirus and software updates on a company issues device?_____
    1. The company's cell-phone carrier
    2. My supervisor
    3. IT Support Department
    4. Compliance Officer
6. I just downloaded a free program online and now my computer is running very, very slowly. Which of the following most likely happened?

    __A. I didn't install the program properly.

    __B. I didn't have enough space on my hard drive for the new program.

    __C. I downloaded spyware and/or adware, too.

    __D. Someone snuck in while the program was downloading and changed my password.
7. What helps prevent your computer from responding to pings (calls) from hackers.
    1. Firewalls
    2. Passwords
    3. Locking my computer
    4. Enabling the screensaver

Cyber Safety Basics – Quiz

8. True or False? It is a good idea to write your password in a post-it note and store in my cabinet.

   __True.

   __False.

9. You are not part of the Finance Department and have never been involved with budget estimates. However, you received an email from your boss with a subject line: For your Urgent Review. It has an attachment titled, BudgetRequest-2018.doc. What do you do?

   __A. Open the email immediately and start reviewing.

   __B. Mark the email for action later.

   __C. Confirm with your boss before acting on it and inform IT Support.

   __D. All of the above

10. You received a call from your financial institution and they asked for your online banking password? What do you do?

    __A. Spell the password.

    __B. Ask for their email address and email the password.

    __C. Disconnect the call and inform your financial institution and IT Support.

    __D. All of the above.

Arizona Priority Care™

One Goal. One Priority. Your Healthcare.

Please click the link below to start the test.

2019 Cyber Security Compliance