CGS®

A CELERIAN GROUP COMPANY

myCGS Security Awareness Training

Length: 12:23
Date Recorded: 10.13.2021

Hello and welcome to the myCGS security awareness video. I'm Maurdi Wilson, a member of your Provider Outreach and Education team at CGS DME MAC Jurisdictions B and C.

Since you may use myCGS, the web portal for DME Jurisdiction B and C suppliers, on a regular basis as part of your job, you need to understand the basics of information security as it applies to your use of this system.

CGS and CMS take security seriously. We have a lot to protect—patient information, supplier information, and your personal information. Medicare fraud and cybercrime are both multi-billion dollar industries. Criminals continue to discover new ways to steal data and to compromise organizations. Being proactive with security efforts is the best way we can strengthen our position to keep our data secure.

Passwords are the first line of defense in the security of almost every computer, website, and mobile device. Because we use passwords so often, we can easily develop bad habits that make our passwords so simple that they are nearly useless.

Managing all of your passwords is a huge challenge. But by following a few simple steps, we can improve security while also making our lives a little easier.

Passwords should always be a combination of symbols, numbers, and mixed-case letters. To create a strong password, try creating a passphrase or group of words that make sense together and are easy for you to remember, but hard for anyone else to guess. Remember, longer passwords are stronger passwords.

For example, you could use a quote from your favorite movie or book, such as "Elementary, my dear Watson." Now take that quote and mix in some symbols, numbers, and a mix of capital and lowercase letters and you might come up with something like this. And an example is provided to you on the screen.

When a data breach does occur, our awareness and response must be timely. If someone does gain access to one or more of your passwords, you have lost some control of your online identity.

You can better safeguard your online identity by following these simple password rules:

Never use the same password for multiple accounts. Every account needs its own unique password.

Never write down or store your passwords somewhere obvious. Consider getting a password manager instead, which is software that stores all of your credentials on your behalf.

Never reveal your passwords to anyone. Keep them secret!

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Don’t use a single word (for example, password), or commonly used phrases like ILOVEYOU. Instead, use phrases that are less common and harder to guess.

Make passwords hard to guess, even by those who know a lot about you.

Never share an ID or account with a coworker. When you set up your myCGS account, be sure that it is your own individual account. Do not use a shared email account to register. All individuals who need access to myCGS must register separately.

myCGS includes strict password requirements in order to ensure that all users have a strong password. Passwords in myCGS must:

Be at least eight characters

Begin with a letter

Include at least one upper case letter

Include at least one lower case letter

Include at least one number

Include at least one special character (such as @,#, or $, etc.)

Contain at least six different characters than your previous password

May not be the same as one of your previous 12 passwords

When you change your password, you cannot reuse any of your previous 12 passwords.

Additionally, your new password must contain at least six different characters than your previous password, or if you reuse the same characters, they must be in a different position within the password. For example, if your previous password started with the letter P, your new password should start with a different character, but you can still use the letter P in a different position of the password.

myCGS does require that your password be changed every 60 days. Your ID will be suspended if you do not log in to myCGS for 30 days, or if your password is entered incorrectly three consecutive times within 120 minutes. Always be sure to keep your myCGS account active and up to date. For additional information about passwords in myCGS, refer to the DME myCGS User Manual.

In addition to passwords, there are other potential security threats that you should be aware of. Let’s take a quick look at a few of these threats.

Malware, such as viruses, spyware, keyloggers, adware, trojans, and ransomware, is an ever-expanding threat to cybersecurity. Research suggests that almost one billion different types of malicious software are roaming around the internet, infecting computers, phones, tablets, and home networks. Use of antivirus and malware detection software is a must in this day and age to protect against these threats.

Be a human firewall. Firewalls are technical controls that manage the flow of data traffic in two directions. They are designed to control what data may leave or enter an organization, allowing legitimate traffic in while keeping hostile traffic out. While firewalls are an effective tool, many security attacks target individuals, which means we need to also be human firewalls by paying attention to the little things in email and social media. Pay attention when websites connect with HTTP instead of the more secure HTTPS in the address bar. Notice when someone asks for more PHI or PII than is needed, and only release PHI/PII that is absolutely necessary.

Be careful on social media, keeping an eye out for scammers. When you respond to an email, be sure that you know who you are responding to.

Social engineering is another type of online scam. More than 90% of successful attacks against organizations worldwide are the result of social engineering. Social engineering comes in many forms, including:

Dumpster Diving. Trash such as phone directories, organization email lists, staff files, medical files, memos, USB sticks, and hard drives are all gold mines for dumpster divers looking to target an organization or individual. That is why it's important to properly dispose of all documents and electronic storage. Use shredders or secure disposal bins.

Phishing is the act of sending fraudulent emails purporting to be from a reputable company in order to induce individuals to reveal personal information, including passwords. More than 90% of data breaches are initiated by phishing attacks, and over 30% of phishing emails are opened, making phishing the most common and effective form of social engineering. Before providing any personal or sensitive information via email, ensure that the email you received is legitimate. Note that emails from CGS are identifiable by their domain name—either cgsadmin.com or mycgsportal.com.

Vishing is similar to phishing, but it's done over the phone. Criminals often call potential victims and pretend to be someone they are not in order to get you to provide them with personal and/or confidential information. Always verify the identity of any caller before giving out any information.

Never give out personal information to anyone unless you know for a fact whom you are dealing with and you agree that they have a legitimate need. And never share your myCGS credentials with anyone, especially your password.

Now that we've discussed some of the threats to your cybersecurity, let's talk about some of the specific rules that you and your company should follow when using myCGS.

Information displayed within myCGS should only be used to conduct Medicare-related business. Information obtained from myCGS should only be discussed with individuals in your organization who have a business need to know the information.

Your physical workstation should be secure. This includes requiring a User ID and password or token to log on to the workstation and securing the workstation when you are not at your desk.

Only use the myCGS MBI Lookup Tool when a Medicare patient can't give you their Medicare Beneficiary Identifier (MBI).

Never use any kind of "bots" or other data-mining software in myCGS. Use of such software will result in the revocation of your myCGS account.

When registering for myCGS, you are required to set a 4-digit PIN. Be sure to keep this PIN safe! Do not share it with anyone, and be certain that you can remember it yourself.

Be sure to follow all of the myCGS password and usage rules discussed earlier in this video to prevent your account from being suspended.

For guidance on how to use myCGS, be sure to consult the myCGS User Manual, Registration Guide, and FAQs found on our website. Links to these educational items are found on the DME myCGS log in page.

After watching this video, myCGS users will be asked to confirm that you have viewed the video and confirm your adherence to our security guidelines. Thank you for watching, and have a great day!