

Security Awareness and CYBER

Guidelines for All CSOC Providers

June 2023 – (02026)

PerformCARE[®]

Delivering
High-Quality
Service and Support

Understand/Recognize:

- Your obligation to protect Personal Health Information (PHI) and Personally Identifiable Information (PII) data in CYBER
- Security Best Practices
 - Using strong password configuration
 - CYBER Password reset functionality
 - Safeguarding passwords / Locking your computer
 - Securing your network
- Public WIFI risks
- What to do if your Network/Computer is compromised
- References

CYBER Login

The CYBER login area has a statement that you acknowledge your responsibility to protect the privacy of and to guard against inappropriate use or disclosure of this PHI by logging in as a CYBER User.

Your CYBER password defends and protects Personal Health Information in CYBER.

CYBER LOGIN

As a CYBER user, I understand that my work will involve access to Protected Health Information (PHI) as defined by HIPAA (The Health Insurance Portability and Accountability Act) for the purpose of providing or arranging treatment, payment, or other health care operations. I also acknowledge that I am engaged by a covered entity. I further acknowledge my responsibility to protect the privacy of and to guard against inappropriate use or disclosure of this PHI by logging in as a CYBER user.

This acknowledgement is in compliance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and its implementation regulations. For more information on HIPAA, please go to <http://www.hhs.gov/ocr/hipaa/>

CYBER contains substance use diagnosis and treatment information that is protected by federal confidentiality rules (42 CFR Part 2). Users that access such confidential information pursuant to a valid written consent are prohibited from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The federal rules restrict any use of the information to criminally investigate or prosecute any person with substance use treatment needs.

Please CLEAR your browser Cache before using this new version of CYBER.

Username

Password

LOGIN

[Customer Service Request Form](#) | [Forgot Password?](#)

© 2024 - CyberAng 1.0.0.455.21-2.0.0.18-10

This statement will appear each time you log in.

Protect PHI/PII

Protected Health Information or PHI should not be shared in email messages unless encrypted.
Do not include youth PHI or potential PHI in email messages to PerformCare.

PHI consists of any health details about a youth associated with identifying information such as:

PHI data in CYBER can include

- Name or Initials of a Name
- Address
- Date of Birth
- Social Security Number
- CYBER ID
- Authorization number
- Medicaid number
- Dates of Service

PII data can include

- Location of birth, race, religion, weight, geographic indicators, employment information, education information, rental applications
- Passport, taxpayer ID, driver's license, or other government-issued ID number
- Facial recognition, fingerprint, handwriting, retinal scans, voice signature, etc.
- Credit or debit card number

The Service Desk Request Form allows you to send inquiries about youth to PerformCare securely: www.performcarenj.org/ServiceDesk

- Keep your computer updated with security, software, and hardware updates
- Use up-to-date, Anti-virus anti-malware software
- Watch out for phishing scams, spyware, and malware
- Don't open suspicious emails or links
- Use strong, complex passwords. First line of defense against unauthorized access to your computer
- Use a trusted secure network or a Virtual Private Network (VPN)
- Back up your data

Never share any passwords with anyone,
not even your CYBER Security Administrator.

Use a strong, complex password.



A strong, complex password:

- Is eight or more characters in length
- Contains both uppercase and lowercase letters
- Contains at least one number
- Contains at least non-numeric (# \$ % & - _)
- Contains non-sequential number or letters
- For CYBER it cannot be a password you have used in the past 4 password cycles
- It should not contain common information (birth dates, pet names, family names, dictionary words, local sport teams, etc.)

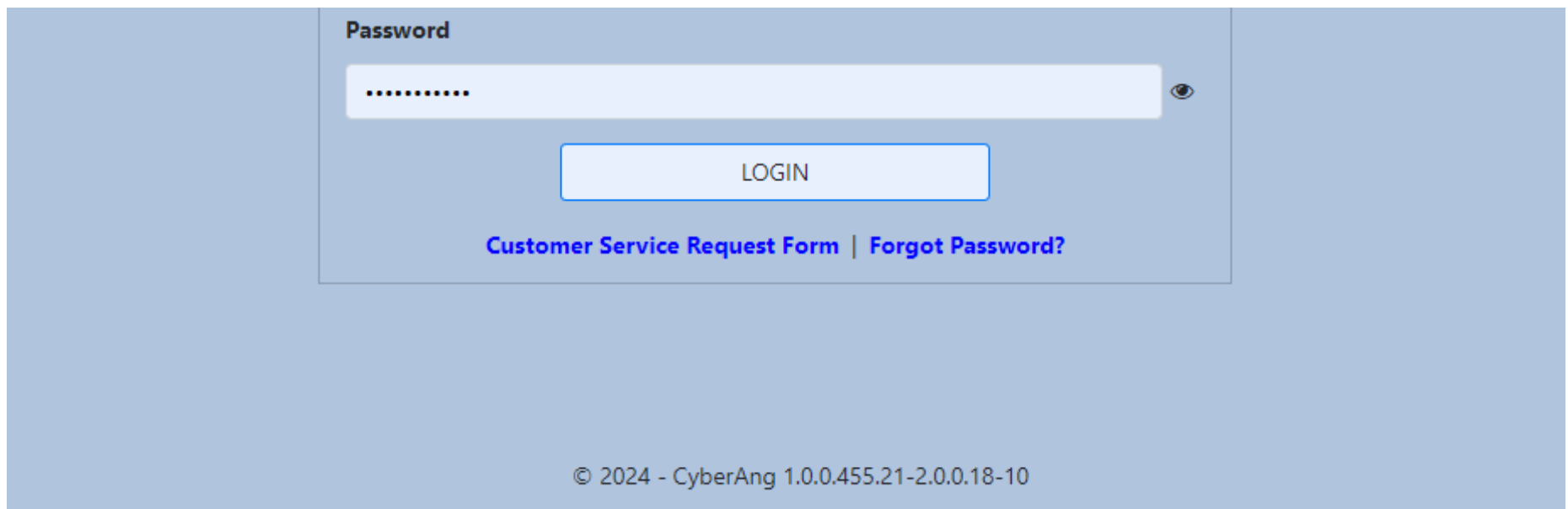
How often should your CYBER password be reset?

CYBER passwords should be reset at least every 90 days or anytime you are locked out.



If you forget your password, you can reset your password without contacting the CYBER Service Desk.

Use the CYBER Password reset functionality.



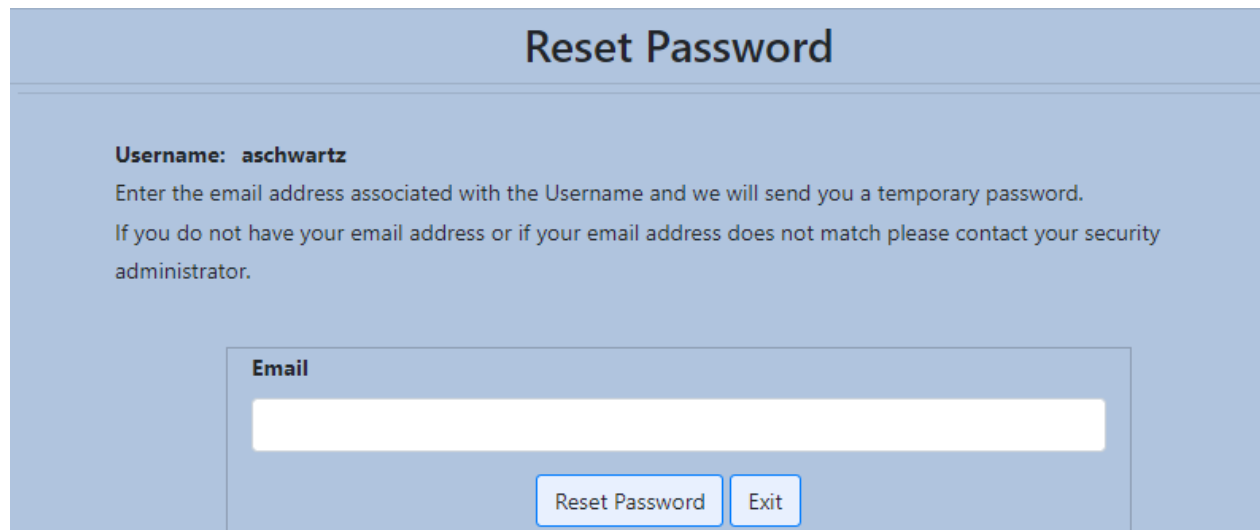
The screenshot shows a login interface with a light blue background. At the top, the word "Password" is displayed in a small, dark font. Below it is a white input field containing a series of dots, representing a masked password. To the right of the input field is a small eye icon. Below the input field is a white button with a blue border and the text "LOGIN" in blue. Below the button, the text "Customer Service Request Form | Forgot Password?" is displayed in a blue, underlined font. At the bottom of the interface, the copyright notice "© 2024 - CyberAng 1.0.0.455.21-2.0.0.18-10" is visible in a small, dark font.

For Password Reset for All Providers, See [Additional Training References](#)

DEMO LOGIN

Reset Your CYBER Password

- Enter the correct Username for the account and enter your password (five attempts to enter the correct Username and password)
 - CYBER will ask for your email associated to that Username.
 - Enter the associated email. (five attempts to enter the correct email)
 - A temporary random password will be sent to the email.
 - Close all browser windows.
 - Copy and paste the random temporary password into the CYBER login screen.
 - CYBER will display a password reset screen.



The screenshot shows a web form titled "Reset Password" with a light blue background. Below the title, it displays "Username: aschwartz". A message instructs the user to enter their email address to receive a temporary password, and provides a contact point for security administrators if the email is missing or incorrect. There is a text input field labeled "Email". At the bottom right of the form are two buttons: "Reset Password" and "Exit".

Reset Password

Username: aschwartz

Enter the email address associated with the Username and we will send you a temporary password.
If you do not have your email address or if your email address does not match please contact your security administrator.

Email

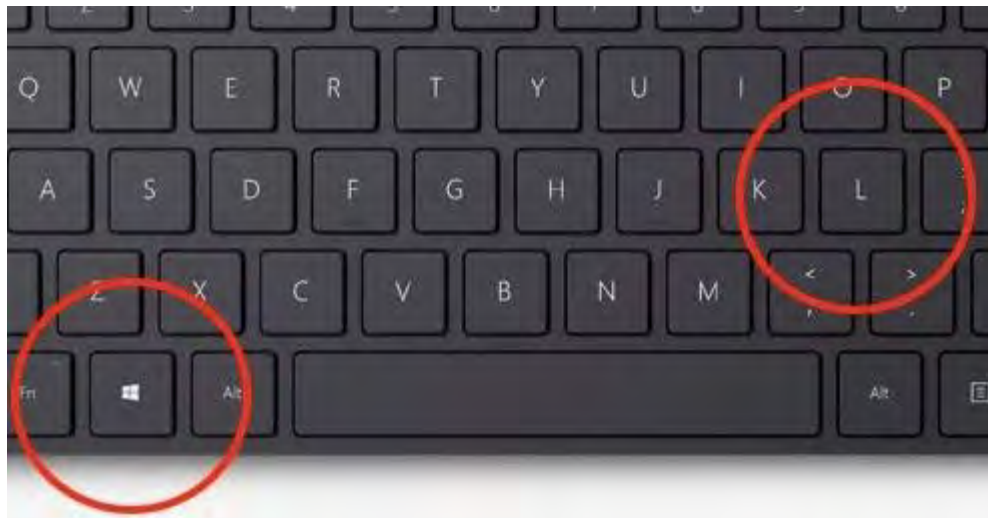
It is extremely important to properly safeguard your password.

- **Do not write down your passwords anywhere.**
- Do not store your passwords in a document on your computer.
- **Never share your passwords with anyone.**
- All of your passwords should be different.

Take a break from working - Lock your screen!

Never not leave your *unlocked* computer unattended at home or in a public place (library, cafe), it is a security risk!

The quickest way to lock a Microsoft screen is to simply **click the Windows Key* + L at the same time.**




*Microsoft PC users

Public WIFI / Hotspots

Public Wi-Fi Hotspots offered at coffee houses, hotels, libraries, airports and other locations, can allow your data to be accessible to others.

Tethering is the term used for connecting devices to the internet using your phone's mobile signal via Bluetooth, or *more securely, using a hard-wired Ethernet or USB cable.*

A cell phone's mobile hotspot can be hacked either at the point where it connects to the internet or the point where it connects to any wirelessly tethered device.



Best Practice Recommendation:

**Do not use a public network if you have more secure options.
Work in a private office with a secured network and/or use a Virtual Private Network (VPN).**

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.

1. Remote-access VPN - VPN that allows mobile employees or remote workers to **access their company's intranet from home or anywhere (CISCO, Check Point, Sophos)**
2. Cloud VPN - VPN technology that's specifically designed for **cloud-based applications and data (Google, Microsoft, and Amazon)**
3. SD-WAN VPN – VPN that works for both on-premise and cloud-based services – **Software-Defined Wide Area Network that ensures end-to-end security (VMWare, Citrix, Lumen, CISCO, Oracle)**

Secure Your Home Office

If you do any work from home, you should ensure that your home office is secure.

- Desk and computer are clear of PHI, screen is not visible to passersby.
- Network is password-secured. Use an Ethernet cable.
- Use headphones when having phone conversations.
- Documents are kept in a locked file cabinet or shredded.
- Do not put passwords on Post-It notes!

Add a complex password to your network and change your password routinely!



If you are aware that your agency network or computer has been compromised, **change your passwords immediately** and then report it to your Security Administrator and contact PerformCare.

Contact PerformCare:
1-877-652-7624

CYBER References

PerformCare Training webpage:

<http://www.performcarenj.org/provider/training.aspx>

Password Reset for All Providers:

<https://www.performcarenj.org/pdf/provider/training/security/instructional-guide-password-reset-all-providers.pdf>

Quick Reference Guide to Secure Email from PerformCare:

<https://www.performcarenj.org/pdf/provider/training/security/quick-reference-guide-to-secure-email.pdf>

CYBER Security Administrator Instructional Guide:

<https://www.performcarenj.org/pdf/provider/training/security/role-based-security-system-admin.pdf>

Additional References

HITECH Act (*Health Information Technology for Economic and Clinical Health*) explained:
Definition, compliance and violations:

- Law that aims to expand the use of electronic health records (EHRs) in the United States
<https://www.csoonline.com/article/3608192/the-hitech-act-explained-definition-compliance-and-violations.html>

How Secure Is My Password? <https://www.security.org/how-secure-is-my-password/>

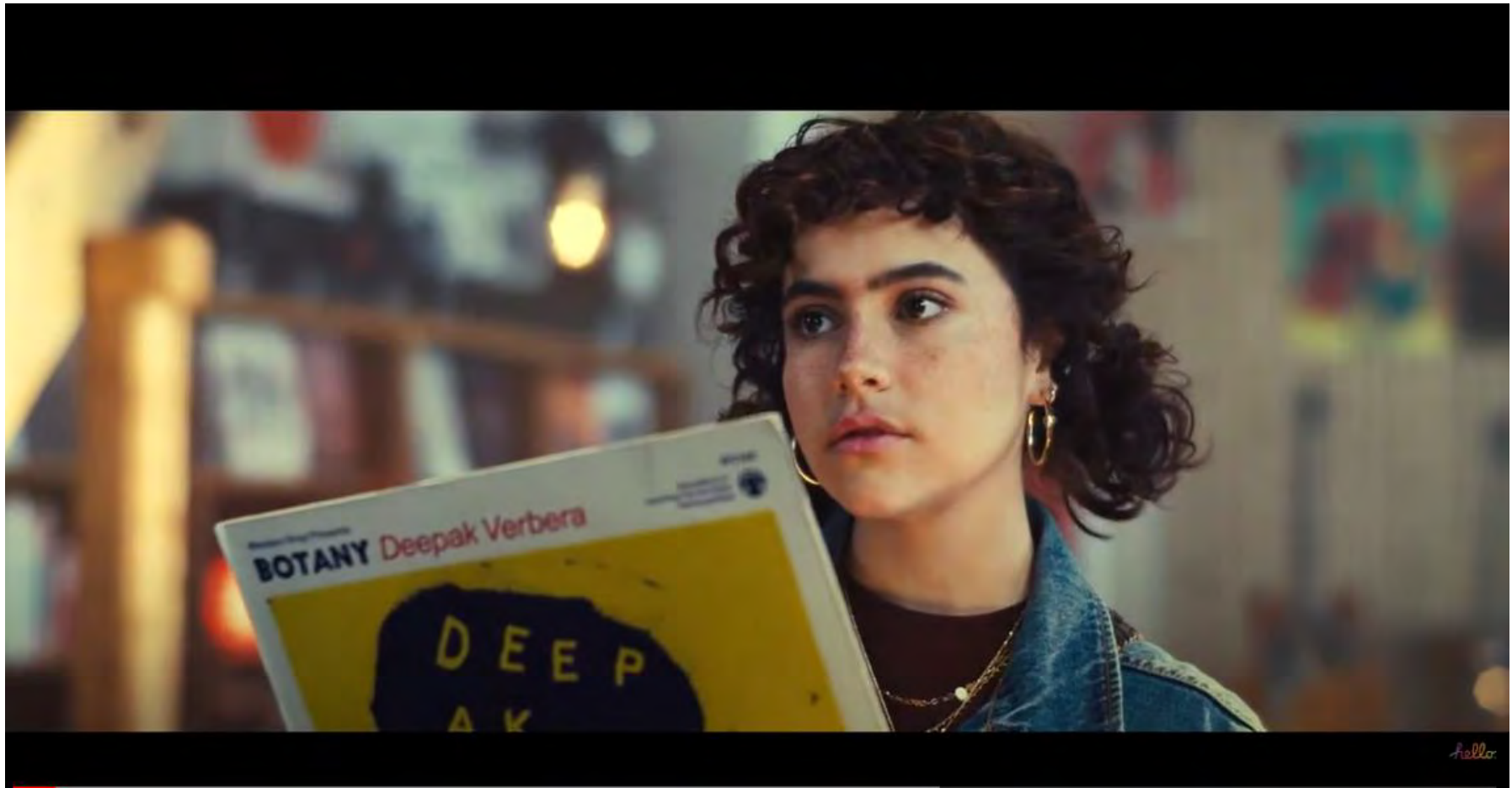
Health Information Privacy: <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>

Forbes - Best Business VPN of 2023 (3/23/2023):
<https://www.forbes.com/advisor/business/software/best-business-vpn/>

Sample - HIPAA Training 101: The Four Rules of HIPAA Compliance (series of videos explaining: <https://www.youtube.com/watch?v=QjKxanDtre0&t=32s>

Protect Your Data

PerformCARE®



<https://youtu.be/4-7jSoINyq4>



Care is the
heart of
our work.

PerformCARE[®]