



Cybersecurity Handbook



Last Updated: Feb 26, 2026

Prepared By: Office of Information Security

Need Immediate Help?

Physical Danger	Local Police: 911 CWRU PD Emergency: (216) 368-3333 CWRU PD Non-Emergency: (216) 368-3300
Service Desk	Call 216.368.HELP (4357)
Information Security	Email askinfosec@case.edu
Technical Support	Visit the CARE Center

Contents

Why Cybersecurity Matters.....	3
Tech Support for Personal & University Devices.....	4
Protect Yourself from Scams & Fraud.....	6
Phishing Scams.....	8
Employment Scams.....	9
Account Security.....	10
Device Protection & Cyber Hygiene.....	12
Back Up Your Files.....	13
Reporting Cybersecurity Incidents.....	14

Why Cybersecurity Matters

In our highly connected world, digital responsibility is a shared mission that protects the entire university community. While we cannot always control data once it has been exposed, we have the power to manage what we share initially. By prioritizing cybersecurity, you play a vital role in safeguarding both your own personal information and the institutional data of Case Western Reserve University. This handbook is designed to empower you with the tools and knowledge necessary to navigate digital threats and maintain robust security habits

Handbook Highlights

- **Tech Support:** Guidance on personal and university device support via the CARE Center.
- **Scam Prevention:** How to identify phishing, employment scams, and immigration fraud.
- **Account Security:** Best practices for Multi-Factor Authentication (MFA) and passphrase management.
- **Cyber Hygiene:** Maintaining software updates, encryption, and safe browsing on public networks.
- **Data Backup:** Choosing between Cloud storage (OneDrive/Google Drive) and full system backups.

Tech Support for Personal Devices

The [U]Tech C.A.R.E. Center

Technical support at CWRU is anchored by the C.A.R.E. Center, your primary destination for hardware and software assistance. Whether you are struggling with a persistent malware infection, experiencing WiFi drops, or need guidance on university-standard software, our technicians are available to provide hands-on help for laptops and desktops. For issues that fall outside our physical scope—such as mobile devices or gaming consoles—or for those who need immediate remote assistance, the [U]Tech Service Desk is available 24/7.

View hours [here](#).

The C.A.R.E. Center will assist with the following requests:

- General troubleshooting
- Hardware replacement on laptops and desktops
- Installing university/academic software
- WiFi and networking issues
- General software and hardware inquiries

The C.A.R.E. Center will NOT assist with the following requests:

- Hardware replacement on phones, tablets, etc.
- Providing temporary chargers or cables
- Custom built desktop PCs

C.A.R.E. Center Location

Kelvin Smith Library
11055 Euclid Avenue
Lower Level
Cleveland, OH 44106

C.A.R.E. Center Loaner Program

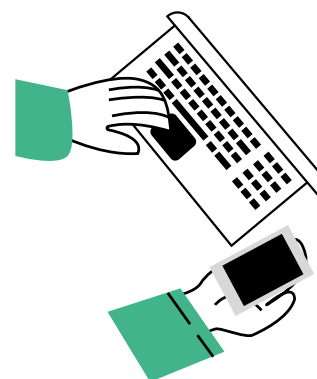
The C.A.R.E. Center offers a free loaner laptop program for students. Receiving a loaner laptop is subject to C.A.R.E. Center approval.

Remote Technical Support

[U]Tech offers unlimited and complimentary 24/7/365 computer service and support to CWRU students, faculty, and staff through the CWRU Service Desk.

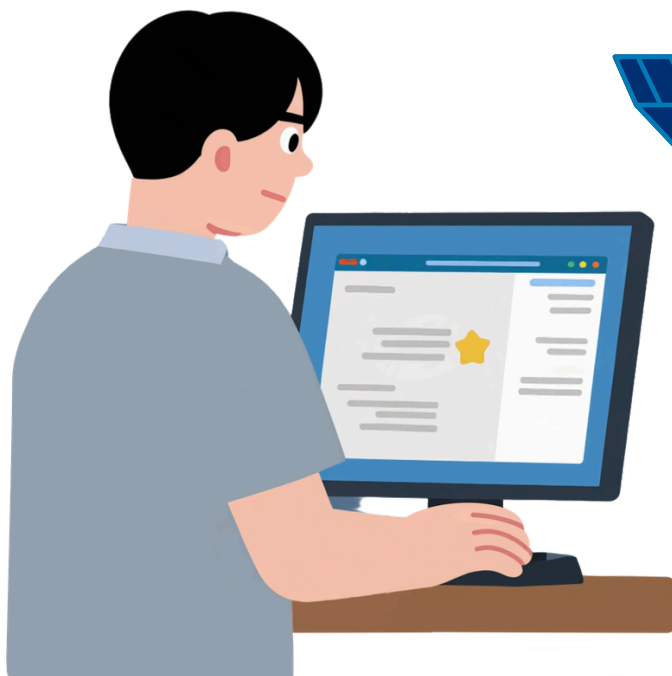
Contact Options:

- Phone Assistance: 216.368.HELP (4357)
- Email: help@case.edu
- Live Chat: help.case.edu



Software Services

CWRU also provides students with licenses for certain educational software through the [Software Center](#).



Visit the [CWRU Software Center](#) for essential university software

Protect Yourself from Scams & Fraud

Cybercriminals do not always 'hack' into systems; often, they simply 'track' users into giving away their keys. Scams today are highly sophisticated, ranging from fraudulent job offers that promise easy income to urgent warnings about your immigration status or bank account. By learning to recognize the hallmark signs of a scam, you become the strongest link in our security chain.

If you suspect you've been targeted, remember: it is always better to pause and verify than to react in haste.

In general, be aware of these risks:

- **Applied Pressure.** Beware of anyone who tries to rush or push you into a decision without thinking twice about it. Don't be afraid to say "no," hang up, or walk away. If you feel uncomfortable, don't engage.
- **Threats of impersonated government agencies.** Attackers know you're likely to respond to representatives or employees of major and popular businesses, brands, or organizations based on blind trust.
- **Sketchy Information.** Always verify information through trusted sources and avoid sharing personal details.
- **Demands for payment.** Never send money without confirming the situation is legitimate. This can include sending money via gift cards, money transfer apps, cash, checks, or cryptocurrency tokens.
- **Lots of grammatical mistakes.** Review emails, messages, and online chats for misspellings, grammatical errors, strange subject lines, or other discrepancies.
- **Promise of easy money.** There is no such thing as guaranteed income, and a promise of seemingly easy money should set off alarm bells.



The **External** Header

Look out for this header in your CWRU email. While not every external email is a scam, most scams come from emails outside the CWRU organization.



Goals of a Scam:

- **Identity Theft:** Using your credit cards and opening accounts in your name to impersonate you.
- **Remote Access to your Computer:** Installing malware can give attackers access to your accounts and personal information.
- **Purchasing Items:** Tricking you into buying gift cards or non-existent goods.
- **Stealing your Money:** Changing your direct deposit details or draining your bank account.



Tips & Best Practices:

- **Beware of Attachments and Links:** Check and hover over links before clicking on them.
- **Check the Sender:** Review the sender's email address to confirm authenticity. Official messages should come from organizational domains.
- **Protect your Credentials:** Never share sensitive information via email, text, or phone. Reputable companies will never ask for it.
- **Limit Public Information:** Share less of your personal life online to reduce the information cybercriminals can use to target you.

Phishing Scams

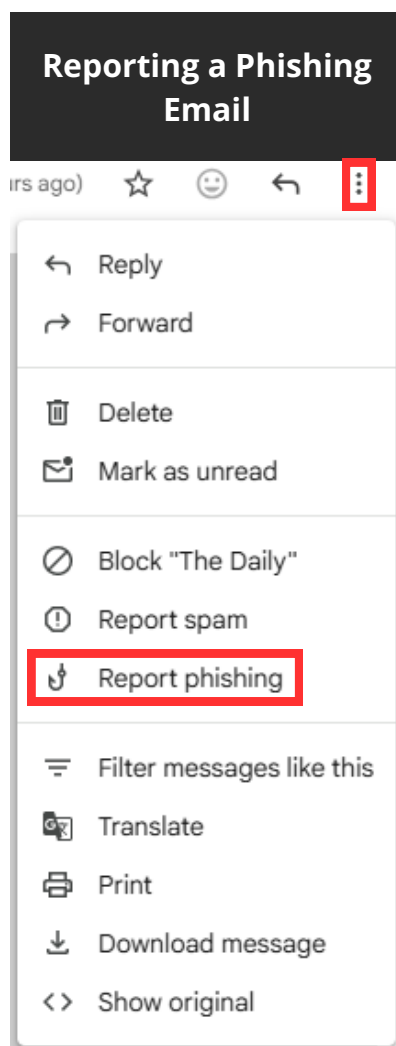
Phishing remains the primary way cybercriminals gain access to university networks. These attacks are designed to look like legitimate communications from CWRU departments, banks, companies, or even your peers. By masquerading as a trusted source, attackers hope you will click a malicious link or provide your login credentials without thinking.



Smishing: Smishing (SMS phishing) is a common attack where scammers send deceptive text messages to lure you into clicking malicious links or revealing personal details



Vishing: Vishing (voice phishing) is a common attack involving fraudulent phone calls or voice messages impersonating trusted authorities that are designed to manipulate you into sharing sensitive information.



Employment Scams

Employment scams are a sophisticated form of social engineering where attackers pose as recruiters, HR managers, or department heads to steal personal information or money. In a university context, these often target students looking for flexible remote work or research assistantships.



Always verify employment opportunities through official company websites. If an offer feels too good to be true (high pay for minimal work with an immediate start), it's likely a phishing attempt. Consult with the Center for Career Success (careers@case.edu) if you need help verifying an opportunity.

How to Avoid Employment Scams

Verify job postings on job boards



Research the recruiter



Protect your personal information



Trust your instincts



Account Security

Your Case Western Reserve University account and credentials allow you access to important services like HCM, SIS, Canvas, and MyHealthConnect. These services contain access to sensitive personal information, including financial, educational, and health records. Practicing safe habits helps prevent misuse of your credentials and protects your reputation and information.

Tips & Best Practices

Use the Duo Mobile App

Set up the Duo Mobile app on your smartphone to get “push notifications.” Find more information here: [CWRU Duo Security](#).



Adopt Duo/MFA Everywhere

You can use Duo for added security on other important accounts, like your personal banking, frequently used accounts, and other accounts with sensitive personal information.

Don't Trust Public Computers

Avoid signing into any accounts on public computers. Only select “Yes, Trust Browser” on computers you regularly use and trust. Never select this option on a public or shared computer. If necessary, use private browsing windows on public computers to prevent your credentials from being saved and close all tabs, clear history, and erase browser cache when done.



Practice Good Password Management

Never reuse your CWRU passphrase for other accounts. Always use different passwords for each account, including your personal accounts. Consider using a password manager to securely store, suggest, and fill your passwords.



Passphrase Management

What is a Passphrase?

Passphrases are a longer sequence of words strung together that can be easier to remember. Since **length is the most critical factor in cryptographic strength**, a long passphrase is significantly harder to crack while being much easier to visualize and remember.



Feature	Password	CWRU Passphrase
Length	Usually 8-12 characters	12-32 characters
Memorability	Low (often requires complex substitutions)	High (can use memorable phrases)
Security	High complexity, less intuitive	Low complexity, more intuitive
Examples	P@ssw0rd!	Hens crossed the ro8d



Don't reuse passphrases or passwords across accounts. Use password managers to help create, manage, and store your passwords securely. Your CWRU passphrase must meet a minimum complexity requirement and cannot reuse the current or last 4 passphrases.



Password Protected

Want to learn more? [Password & Passphrase Security](#).

Device Protection & Cyber Hygiene

Keep your electronics physically and digitally safe from theft or breach.

Use a Password

Protect your devices with complex passcodes, PINs, patterns, or biometrics (fingerprint/facial recognition). If a device comes with a default password, change it immediately.

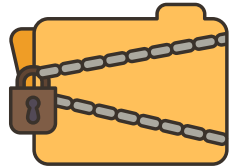


Lock Your Devices

Adjust your device's settings to automatically lock the screen after a certain period of inactivity. Shorter is better, especially for smartphones and tablets, to protect against unauthorized users on your devices.

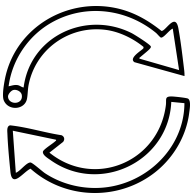
Encrypt Your Devices

Encryption scrambles your data so only you can access it. Ensure that encryption is enabled on all of your devices. Modern computers support hard drive encryption, and most phones are encrypted when you set a passcode. For more information: [Full Disk Encryption](#)



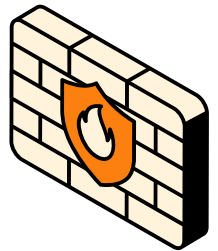
Keep all Apps & Software Updated

Regularly update and restart your devices and applications to fix security vulnerabilities and improve your experience. Only download apps/software from reputable sources like Google Play, Apple App, and Microsoft Store. Do not grant permissions (microphone, camera, location, etc.) to apps that don't need them.



Protect Your Devices

Most modern devices have a built-in antivirus and firewall to protect you from malicious code and items on other networks like the Internet. Ensure that these forms of protection are enabled to add an extra layer of protection.



Browse Safely

Never allow your devices to connect to a network without your permission. Never share or access sensitive information on public, potentially insecure, Wi-Fi networks. Be mindful of websites that may track your activity and collect personal data. Review privacy policies and terms and conditions, and consider using a [VPN](#) or hotspot again.



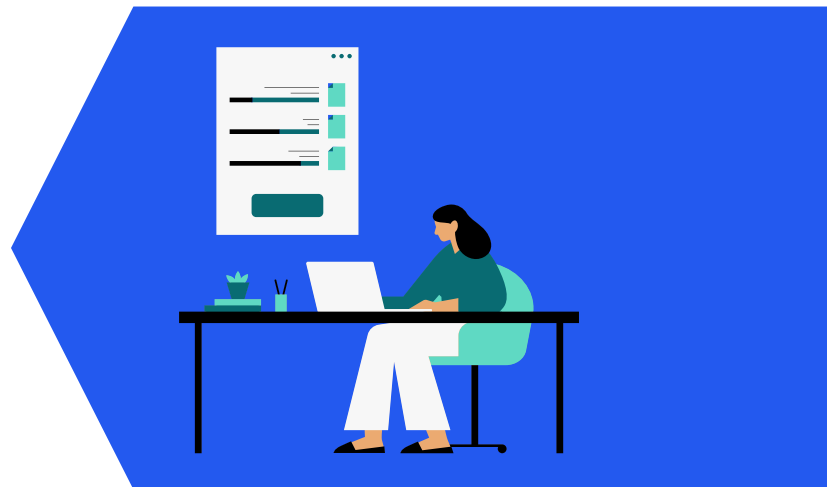
Back Up Your Files

A backup is an extra copy of your digital files that protects against data loss from device failure, theft, corruption, or malware.

Sync/Cloud Options

Sync/cloud services back up individual files, not applications or programs. 1TB of OneDrive storage is offered to all CWRU students and faculty.

For more details: [OneDrive for Individual Storage](#)



Traditional Backup

Traditional backups allow for full system restores, including programs and settings. Using an external hard drive and programs like [Time Machine for MacOS](#) and [Windows Backup](#) can capture all data and applications.

Reporting Cybersecurity Incidents

What might a cybersecurity incident look like?

- Losing a university-owned device
- Discovering malware on a device
- Entering your CWRU credentials into a malicious website
- Falling for a phishing attack
- Research data theft



If you're worried your account may be compromised or need help securing it, contact [U]Tech through one of the following options:

Service Desk	Call 216.368.HELP (4357)
Information Security	Email askinfosec@case.edu
Technical Support	Visit the CARE Center

IMPORTANT:

If your incident poses an immediate danger, contact CWRU PD immediately at (216) 368-3333 or call 911.