UCF Cyber Safety Guide

Table of Contents

Table of Contents

Introduction to Cybersecurity

Cybersecurity is the process of protecting devices, data, networks, and accounts from digital attacks and breaches. In a university environment like UCF, students rely heavily on technology for coursework, finances, and communication. Due to this, students are frequently targets for cyber threats.

The purpose of this cybersecurity guide is to help UCF students understand common cybersecurity risks and learn precautionary measures to protect their devices, data, and personal information.

In this guide, we will first explain key cybersecurity concepts, then identify common threats targeting students, and finally provide step-by-step measures to stay safe online.

What is Cybersecurity

Cybersecurity — The digital protection of devices, data, networks, and accounts from digital attacks and breaches.

Cybersecurity effects how students:

- Submit coursework
- Store and share personal, academic, and financial information
- Communicate through university systems

Cybersecurity effects how students submit coursework, store personal and financial information, and communicate.
In other words, cybersecurity plays a role in every part of a students life.

Why Cybersecurity Matters for University Students

Key Benefits of Cybersecurity:

- Protects personal, academic, and financial information from being stolen.
- Prevents unauthorized access to student accounts.
- Helps build awareness for online security risks.
- Reduces the risk of being victim to phishing, malware, and credential theft attacks.
- Allows students to use university technology safely and confidently.

University students rely primarily on university digital systems, making cybersecurity awareness essential for preventing potential threats. **Before learning how to protect ourselves, it is important to understand the types of risks that students face.**

Current Cybersecurity Risks

Cyber threats that target students are increasing rapidly.

Common threats:

- Phishing — Emails that resemble official university communications used to steal personal data and student passwords.
- Malware — Unsafe links and attachments used to collect data or control student devices.
- Credential Theft — The use of stolen information and data to access student accounts.

These cybersecurity threats are commonly used to steal personal data, passwords, financial records, and unauthorized access to student accounts. Students are a common target of this due to the use of public Wi-Fi, open networks, and large information stored in university databases. **Now that we understand the common threats targeting students, the next section explains how this guide will help you address these risks.**

Purpose of This Manual

This manual will provide task-based guidance on securing student cyber safety while identifying common cyber threats.

The goal of this guide is to give UCF students practical and easy to follow measures that they can apply immediately.

Areas of focus:

- Account security
- Authentication
- Threat recognition
- Network safety
- Password Management
- Data protection

Purpose of This Manual (Cont.)

The remainder of this document is separated into three main sections:

1. **Cyber Threat Awareness and Identification** — how to recognize risks and suspicious activity
2. **Preventative Measures for UCF Students** — step-by-step measures to secure accounts, data, and devices
3. **Security Habits & Resources** — how to maintain cybersecurity practices

Why Students Need Cyber Awareness

Why students need cyber awareness:

- University students are primary targets to cyber attacks.
- There’s a high use of email and university systems for students.
- Being prepared for possible cyber attacks protects personal data and devices.

Cyber awareness helps students safely navigate technology without fear of attacks.

With this foundation in place, we now move into Cyber Threat Awareness and Identification, where we will explore how to recognize and prevent real cyber threats.

Cyber Threat Awareness and Identification

Identifying the cyber threats targeting college students, recognizing the warning signs, and knowing how to respond.

Common Cyber Threats Targeting Students

Key stat: Education is the 3rd most targeted industry by cyber threat actors. Over 90% of universities reported a breach in the past year.

Phishing — Fraudulent emails, texts, or fake websites designed to steal login credentials. Job offer scams and QR code traps are increasingly common on campuses.

Ransomware — Malware that locks files or systems and demands payment. 251 attacks hit educational institutions globally in 2025, exposing 3.9 million records.

Social Engineering — AI-generated emails and voice messages that impersonate staff, professors, or campus departments to manipulate students into giving up information.

Credential Theft — Attackers target student login information to access university systems. 60–70% of cybersecurity incidents involve compromised credentials.

Real-World Examples of Cyberattacks

PowerSchool Breach (2025) — A 19-year-old hacked and extorted the student information system provider for $2.85M. Sensitive data of 10 million teachers and 60+ million students was leaked. Over 100 school systems sued.

Oracle Exploit in Higher Ed (2025) — A software vulnerability impacted 3.5M records at the University of Phoenix, ~100K at Dartmouth College, and 46K at the University of Pennsylvania.

Stanford Fake Job Scam — A phishing email posed as Stanford's Office of the Registrar, offering a fake paid internship with the Bill Gates Foundation to steal student credentials.

Wisconsin University Phishing — Students and staff received phishing emails through Office 365. Recipients clicked malicious links and lost significant sums of money from the scams.

Warning Signs to Look Out For

Urgent or Threatening Language — Messages demanding immediate action like "Your account will be suspended" or "Act now or lose access."

Suspicious Sender Addresses — Official UCF emails always come from @ucf.edu. Watch for lookalike domains like ucf-support.com.

Requests for Personal Information — UCF will never ask for login credentials or passwords via email. Any such request is a red flag.

Suspicious Links or Attachments — Attackers register lookalike domains (e.g., microscft-login.com). Always hover before clicking.

Too-Good-to-Be-True Offers — Fake job offers and paid internship scams are a growing trend targeting college students.

Fewer Spelling Errors Than Before — AI has made phishing emails more polished. Don't rely on typos alone to spot a scam.

How to Know if Your Account Is Compromised

Can't Log In — Your password no longer works, even though you didn't change it.

Unknown Sent Messages — Emails or texts sent from your account that you didn't write.

Changed Account Details — Your email, phone number, or direct deposit info has been altered in myUCF without your knowledge.

New Inbox Rules — Attackers create rules that auto-delete incoming emails so their access goes undetected longer.

Unfamiliar Login Activity — Alerts about logins from devices or locations you don't recognize.

Breach Databases — Check HaveIBeenPwned.com to see if your email has appeared in known data breaches.

Reporting Suspicious Communication at UCF

Step 1: Use the Phish Alert Button — In Outlook, click the "Phish Alert" button to report the email directly to UCF's Security Incident Response Team (SIRT). The message is automatically removed from your inbox.

Step 2: Forward to SIRT — If you don't have the Phish Alert button, forward the suspicious email as an attachment to SIRT@ucf.edu.

Step 3: Contact UCF Info Security — For questions or concerns, email infosec@ucf.edu or call 407-823-2711.

Step 4: If Personally Threatened — Contact UCF Police immediately at 407-823-5555.

Step 5: If You Clicked a Link — Report to SIRT immediately. Change your password right away. Run a malware scan and monitor your accounts.

What Can You Do to Protect Yourself?

Your data is a high-value target. Student identities, financial aid records, and health information are actively sought on the dark web.

Key stat: 60–70% of cybersecurity incidents involve compromised credentials.

Up next: Preventative Measures for UCF Students

Preventative Measures for UCF Students

Before you begin ensure you have the necessary tools and access ready. This guide is designed for beginners and does not require advanced technical knowledge.

01

Hardware Ready

Have your laptop or smartphone charged and available.

02

Stable Connection

Ensure you have reliable internet access to complete setup.

03

Credentials

Locate your UCF NID and login credentials before proceeding.

Pro Tip: Keep your NID secure and never share your password with anyone, including UCF staff.

Step 1: Create Strong Passwords

Strong passwords make it significantly harder for attackers to use automated tools to guess credentials. A unique password ensures that if one account is compromised, others remain secure.

01

Avoid Common Phrases

Skip "123456", "password", or birthdays which are easily guessed.

02

Length & Complexity

Use 12–16 characters with mixed case, numbers, and symbols (!@#$).

03

Passphrase Method

Combine words for security. Example: "KnightsRideAtSunset2026!"

04

Password Manager

Use a manager to store unique credentials and prevent reuse.

Pro Tip: Never reuse the same password across multiple accounts to isolate security risks.

Step 2: Enable Multi-Factor Authentication

MFA adds an extra layer of security by requiring a second verification step beyond your password, serving as a primary defense against unauthorized access.

01

Access Settings

Log in to UCF and navigate to security settings.

02

Enable MFA

Locate MFA Security and follow prompts to register your device.

03

Choose Method

Select push, text, or app code for verification.

04

Verify Status

Confirm MFA is enabled to secure your account.

Why This Matters: Even with your password, attackers cannot access your account without this second factor.

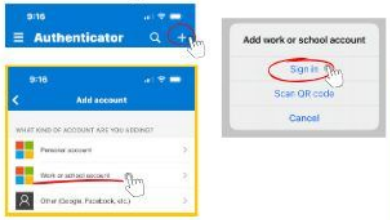
Staff & Faculty Transition to Microsoft Authenticator

Multi-Factor Authentication for UCF

Getting Started:

1 *Download the Microsoft Authenticator app on a personal smart device (phone, tablet etc.)*

2 *Open the app, select + and "Add work or school account" then select "Sign In"*

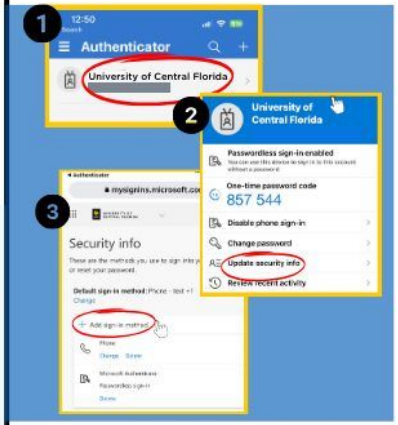


3 *Sign in using your NID@ucf.edu email address and NID password*

4 *Register your device by selecting "Register" and then select "Finish"*

Helpful Tips:

Make sure you add more than one sign-in method for your Microsoft Authenticator app to easily log in to a new device if you don't have the password handy.



<u>Do not delete</u> the Microsoft Authenticator app from your phone. If you delete the app, you may have to re-download the app and re-register your device to access webcourses@UCF (Canvas), your UCF email and more.

Encountering technical issues? Visit https://go.ucf.edu/MFA2024 for more info.

Still need help? Contact IT Support:
Phone: 407.823.5117 | Email: ITSupport@ucf.edu | Submit a Ticket

UCF | Information Technology

Step 3: Practice Safe Internet Browsing

Students frequently browse the internet for academic and personal use, making them prime targets for phishing attacks and malicious websites.

01

Check URLs Carefully

Look for "https://" and a secure lock icon before clicking.

02

Avoid Suspicious Links

Don't click links in messages that urge immediate action.

03

Verify Sender Address

Check for official university domains (e.g., ucf.edu).

04

Official Sites Only

If unsure, visit the official website directly.

Why This Matters: Recognizing suspicious behavior prevents attackers from gaining sensitive information via phishing.

Step 4: Secure Your Devices

Hardening your hardware is a critical step in preventing unauthorized physical and digital access to your personal data.

01

Auto-Updates

Enable updates for OS (Windows, macOS, iOS, Android) to patch vulnerabilities.

02

Antivirus Softare

Install reputable security software to detect and block malware.

03

Strong PIN/Biometrics

Use complex passwords and fingerprints/FaceID. Avoid "0000" or "1234".

04

Access Hygiene

Turn on screen lock and avoid apps from untrusted sources.

Why This Matters: Your device is the gateway to your identity. Physical security and software updates form the first line of defense against compromise.

Step 5: Stay Safe on Public Wi-Fi

Public Wi-Fi networks (such as those in cafes, airports, or libraries) are convenient but often insecure.

01

Avoid Sensitive Accounts

Don't access banking or school portals on public networks.

02

Use a VPN

Encrypt your connection to secure your data from interceptors.

03

Disable Auto-Connect

Prevent your device from joining unknown networks automatically.

04

Verify & Logout

Confirm network names and always log out after use.

Why This Matters: Public networks can be monitored by attackers to intercept your data. Taking precautions prevents unauthorized access.

Step 6: Protect Personal Information

Oversharing online makes you a target for identity theft. Control your digital footprint to stay secure.

01

Privacy Settings

Limit who sees your posts. Review social media visibility monthly.

02

Hide Sensitive Info

Never share your full address, phone number, or Student ID publicly.

03

Email Separation

Use separate emails for school/work and personal accounts.

04

Active Monitoring

Regularly check for unusual activity and be wary of online forms.

Why This Matters: Attackers impersonate victims using social media data to guess security questions. Limiting exposure significantly reduces this risk.

Conclusion: The Importance of Cybersecurity

Cybersecurity is not just a technical issue, it is a daily responsibility that affects every students digital accounts. From accessing student accounts to communicating via email, students rely on technology in nearly every aspect of their academic lives.

Conclusion: The Importance of Cybersecurity Cont.

With access comes risk including data breaches, identity theft, and unauthorized account use. Understanding and practicing cybersecurity helps protect not only personal information but also the broader school community.

Conclusion: The Importance of Cybersecurity Cont.

By staying informed and aware of the many methods used to conduct cyber attacks, students can reduce these risks and contribute to a safer digital environment for everyone.

Conclusion: Student Responsibilities

Each student plays a critical role in maintaining a secure digital environment. Protecting personal student accounts is one of the most important responsibilities a student has online. This includes creating strong and unique passwords, keeping login information private, and being cautious about where and how accounts are accessed. Small actions such as logging out of shared devices or avoiding suspicious links, can make a significant difference. Cybersecurity is most effective when every individual takes ownership of their role in keeping their information secure.

Conclusion: Proactive Security Habits

Good cybersecurity is built on consistent, proactive habits. Rather than reacting to problems as they occur, UCF students should take steps to prevent issues before they arise. This includes:

- Staying aware of suspicious sender addresses that imitate UCF domains.
- Reporting requests for personal information.
- Avoiding suspicious URLs or attachments.
- Detecting domains imitating Microsoft or UCF addresses.
- Knowing what a phishing attack looks like.
- Logging out of accounts on shared devices.
- Avoid accessing accounts holding private information on public networks.

Support Resources

Knowing where to turn for assistance is just as important as preventing cyber attacks. If a student suspects that their account has been compromised, encounters suspicious activity, or is unsure about a potential threat, they should report it immediately. As provided previously in this guide, here are some support resources that are provided for UCF students when in need of assistance:

- UCF Information Security (InfoSec) - https://infosec.ucf.edu/about-us/#Contact
- UCF Security Incident Response Team (SIRT) - https://infosec.ucf.edu/sirt/
- Identity and Access Management (IAM) - https://infosec.ucf.edu/identity-management/
- Risk and Compliance - https://infosec.ucf.edu/risk-and-compliance/
- Security Awareness - https://infosec.ucf.edu/awareness/

Final Statement

Cybersecurity is an ongoing commitment, not a one-time task. As technology continues to evolve, so do the risks associated with it.

Final Statement Cont.

By staying informed, taking responsibility, and practicing strong digital habits, students can confidently navigate through their accounts without having to worry about their information being stolen.

Final Statememement Cont.

Through the knowledge and skills learned in this guide, cybersecurity awareness will remain valuable far beyond school accounts, supporting personal safety and future success while accessing the digital world.

Colophon

This document was prepared by the following project team:

Project Manager/Editor

Raphael Losada

Writers and Designers

Dillon Madascy

Yasmin Mouloula

Specialist/Primary Writer

Joseph Bedrous

Tools and Production

This document was written and collaboratively edited using Google Docs. Visual Layouts and original graphic elements were created using Adobe Express.

Templates and Unoriginal Visual Assets:

Document templates and select visual elements may include third-party resources.

Template and visual asset attributions:

Works Cited

Awareness Information Sources

Stevens, Emma. (2025). *Top 10 cyber threats facing the education sector*. BitSight. https://www.bitsight.com/blog/top-10-cyber-threats-facing-education-sector

Rahn, Don. (2025). *Top cyber threats to educational institutions*. Blackbaud. https://blog.blackbaud.com/top-cyber-threats-to-educational-institutions/

Rahn, Don. (2026). *Top cybersecurity risks facing educational institutions (2026)*. Blackbaud. https://blog.blackbaud.com/top-cybersecurity-risks-facing-educational-institutions-2026/

Sourwine, Abby. (2026). *Cyber attacks on schools plateaued in 2025, but more records exposed*. Government Technology. https://www.govtech.com/education/cyber-attacks-on-schools-plateaued-in-2025-but-more-records-exposed

Times Higher Education. (2026). *Cybersecurity threats to universities and colleges: How to stay safe*. Times Higher Education. https://www.timeshighereducation.com/campus/cybersecurity-threats-universities-and-colleges-how-stay-safe

Works Cited

Awareness Information Sources (Cont.)

Mendez-Padilla, Briana. (2025). *Ransomware attacks on education jump 23 percent in H1 2025*. Higher Ed Dive. https://www.highereddive.com/news/ransomware-attacks-education-jump-23-percent-h1-2025/754011/

Sourwine, Abby. (2026). *Cyber attacks on schools plateaued in 2025, but more records exposed*. Government Technology. https://www.govtech.com/education/cyber-attacks-on-schools-plateaued-in-2025-but-more-records-exposed

Stanford University IT. (2023). *Phishing scams often target Stanford students*. Stanford University. https://uit.stanford.edu/news/phishing-scams-often-target-stanford-students

Miller, Emily. (2026). *The state of higher education cybersecurity: Insights & trends*. BitLyft. https://www.bitlyft.com/resources/the-state-of-higher-education-cybersecurity-insights-trends

Morrow, Ethan. (2024). *[Article on phishing email characteristics and detection]*. ScienceDirect. https://www.sciencedirect.com/science/article/pii/S0747563224001420