

October 2026

Priority Level: High

Threat Overview: Student Loan Phishing And Account Takeovers

High school seniors, recent graduates, parents, and school staff are increasingly targeted by phishing campaigns impersonating schools, colleges, scholarship organizations, the U.S. Department of Education, and financial aid providers. These scams succeed because students expect messages about admissions, FAFSA, scholarships, and student aid. The broader threat continues to grow. The FBI's Internet Crime Complaint Center (IC3) received more than 1 million cybercrime complaints in 2025, with reported losses exceeding \$20 billion. Phishing and spoofing remain among the most common attack methods, making credential theft a fast path to compromising student accounts and personal information.

Threat Vectors To Watch:

- **Student Loan & Financial Aid Phishing:** Scammers impersonate the U.S. Department of Education, loan servicers, and scholarship organizations to steal FSA IDs, passwords, and personal information.
- **Lookalike School Websites:** Attackers register domains that closely resemble legitimate school websites, changing a single letter or number to trick users into entering their credentials.
- **Account Takeovers:** Stolen credentials allow attackers to lock users out of accounts, access school systems, and impersonate students or staff.
- **Scholarship & College Admission Scams:** Fraudulent scholarship offers, admissions messages, and financial aid notifications can pressure students into sharing personal information or making payments.
- **Sensitive Student Data:** Schools store valuable personal information that can be exploited for identity theft, fraud, or future social engineering attacks.

GOAL: The goal of this campaign is to help schools, students, parents, and staff recognize student loan phishing and account takeover tactics. High school seniors and recent graduates are frequently targeted because they expect legitimate messages about college admissions, FAFSA, scholarships, and financial aid. Verifying requests through official channels, protecting credentials, enabling MFA, and reporting suspicious activity can significantly reduce risk and help protect student accounts, personal information, and access to essential educational services.

Remember: Security is a Shared Responsibility

- ✓ When in doubt, verify through official internal channels before interacting with unexpected requests.
- ✓ If you click on a suspicious link or enter credentials on a suspicious website, notify your security operations center or responsible IT support immediately.



For more information, scan the QR code or visit
ransomwareinfo.oregon.gov



CYBER READINESS TIPS

Best Practices For Schools

- **Enable MFA** for staff and eligible student accounts wherever possible.
- **Monitor for unusual account activity** to identify compromised accounts early.
- **Vet third-party vendors and EdTech tools** for Family Educational Rights and Privacy Act (FERPA) and Children's Online Privacy Protection Act (COPPA) compliance.
- **Provide phishing awareness training** before Free Application for Federal Student Aid (FAFSA), scholarship, and graduation seasons.
- **Maintain tested backups** of critical systems and student records.
- Provide clear reporting channels for **suspicious emails and account activity**.

Helping Students Stay Safe Online

- **Teach students to verify financial aid messages** through official school or Federal Student Aid channels.
- **Warn seniors about student loan scams** before graduation and FAFSA deadlines.
- **Help families recognize official websites** before entering student information.
- **Encourage immediate reporting** of suspicious emails, texts, or account activity.
- **Support digital citizenship education** that helps students recognize phishing, impersonation, and online scams.
- Remind students that **legitimate organizations won't ask for passwords or FSA IDs by email or text**.

Questions For Schools

- Do we monitor for **unusual account activity**?
- Can we quickly identify **compromised student accounts**?
- Are we reviewing **third-party applications** connected to school accounts?
- Do students and staff know **how to report phishing**?
- Are we communicating about **student loan scams** to students and families?
- Are we regularly testing our **incident response procedures**?
- How are we achieving **defense in depth**?

Protect Your Student Accounts

- Use **strong, unique passwords** for school and personal accounts.
- Turn on **MFA** wherever it is available.
- **Never share your FSA ID, passwords, or verification codes**.
- Go directly to **official school or Federal Student Aid websites** instead of clicking unexpected links.
- Review **account recovery information regularly** to ensure phone numbers and email addresses are current.

Additional Resources:

Oregon Emergency Response System
(OERS) 1-800-452-0311

Cybersecurity & Infrastructure Security Agency (CISA)
888-282-0870 | www.cisa.gov

FBI Field Office - Cyber Task Forces
Portland Office 503-224-4181
<https://www.ic3.gov/>
fbi.gov/contact-us/field

Multi-State Information Sharing and Analysis Center®
(MS-ISAC®) 866-787-4722

State of Oregon Security Operations Center
503-378-5930 | css.soc@eis.oregon.gov

National Institute of Standards and Technology (NIST)
<https://www.nist.gov/cybersecurity-and-privacy>



For more information on strengthening your cybersecurity posture, refer to the FBI's Operation Winter SHIELD guidance.

<https://www.fbi.gov/investigate/cyber/wintershield>

