

Internet Crime Complaint Center (IC3)

Published: 2026-05-15 · Archived: 2026-08-06 02:02:04 UTC

The Federal Bureau of Investigation (FBI) is providing this Public Service Announcement (PSA) to warn of potential future impacts related to a cyber-attack that affected an online Learning Management System (LMS), resulting in an interruption of service to educational institutions and students across the country. The LMS platform is now fully operational.

ShinyHunters (SH) — which claimed the cyber-attack that caused the disruption—is a cyber criminal group specializing in large — scale data breaches and extortion. They target major companies across tech, finance, and retail, often stealing millions of customer records at once.

Threat actors often use their real or exaggerated claims of access to sensitive or personal information to prompt payment from victims. Victims may receive an extortion email signed as *ShinyHunters*. To exert pressure on victims¹, SH actors commonly use harassment strategies, sending threatening text messages and phone calls to victims and their family members, and in some cases, swatting². Threat actors may falsely claim to have sensitive or compromising information, including embarrassing photographs or videos of victims, which frequently do not exist. Following these pressure tactics, SH actors have sometimes posted exfiltrated data to various iterations of the SH data leak site on the Tor network.

Educational institutions with exposed cloud-based management platforms, integrated third-party services, and access to sensitive customer or enterprise data are at an elevated risk. The compromise of sensitive customer or enterprise data could allow threat actors to craft highly sophisticated spearphishing³ campaigns using real-world context to deceive students and faculty. SH actors' access to sensitive data could provide them an opportunity to sell the stolen data to other cyber criminals or reuse stolen data from education platforms to impersonate school faculty, IT support, financial aid offices or others in future attacks.

Recommendations

The FBI understands the concerns of individuals and students impacted by recent SH activity. The FBI strongly recommends individuals await formal guidance from educational institutions regarding the scope of the incident and the nature of any affected data. Furthermore, the FBI recommends individuals consider the following actions if contacted directly by anyone claiming to have your personal data:

- Verify urgent or unusual requests received through emails, texts, calls via another communication method before responding.
- Do not send payment or respond to their demands.
- Remain cautious of unsolicited emails, calls, or texts claiming to be from your school, the LMS provider, or law enforcement.
- Verify all contacts through existing and known channels before responding.
- Do not click on suspicious links or download unexpected attachments.

Victim Reporting and Additional Resources

For an immediate, life-threatening emergency, dial 9-1-1.

The FBI encourages any suspected SH intrusions to be reported to the FBI Internet Crime Complaint Center at www.ic3.gov or their local FBI field office at www.fbi.gov/contact-us/field-offices or [1-800-CALL-FBI](https://www.fbi.gov/1-800-CALL-FBI) (225-5324).

- Retain all the information regarding the incident (i.e. usernames, email addresses, monikers, websites, platforms used for communication, names, photos, videos, etc.).
- When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

If you or someone you know may be a victim of a crime using the tactics outlined above, the following resources may help:

- Consult a health care provider who can provide an initial evaluation or referral to a mental health professional.
- Connect to a mental health resource who can help learn health coping skills for intense emotions and help reduce the risk of serious injury.
- Contact your account providers immediately to regain control of your accounts, change passwords, and place alerts on your accounts for suspicious login attempts and/or transactions.
- Visit fbi.gov for more resources on coping with the impact of crime:
 - www.fbi.gov/how-we-can-help-you
 - www.fbi.gov/file-repository/vsd/coping-with-crime-one-pager-april-2026.pdf/view

¹Unless otherwise stated, the use of the term "victim" in this product does not imply that the individual or entity meets the definition of "victim" in the Victims' Rights and Restitution Act (VRRRA), 34 U.S.C § 20141 or the Crime Victims' Rights Act (CVRA), 18 U.S.C § 3771, or that the individual or entity has been identified as a victim in an FBI investigation.↵

²*Swatting* is the act of reporting a false emergency situation with the intention of eliciting a law enforcement or SWAT response.↵

³*Spearphishing* is a highly targeted form of cyberattack where cyber criminals send personalized, fraudulent messages to trick specific individuals into revealing sensitive information, installing malware, or transferring money.↵