Education

Risk Insights

Provided by [B_Officialname]

Phishing in Schools: Training Teachers and Staff to Spot Common Scams

Phishing is a type of cyberattack in which cybercriminals deceive individuals into revealing sensitive information. Educational institutions are a prime target for these scams as they process a wide range of confidential information, including student records, human resources data and financial documents and rely heavily on digital platforms for many key operations. Many schools are also vulnerable to phishing attacks due to limited IT resources and inadequate cybersecurity budgets. Additionally, according to IBM's 2025 Cost of a Data Breach Report, the education industry had an average breach cost of around $3.80 million.

With these risks, training teachers and staff to recognize and report phishing is an essential strategy to strengthen cyber defenses and protect the school community. This article provides more information on common phishing scams and their consequences and describes the signs and red flags of phishing communications. It also offers tips on training school personnel to prevent these events and on how to build a phishing-resistant school culture.

Common Phishing Scams That Target Schools

Cybercriminals often employ these common phishing attacks when targeting educational institutions:

- Impersonation of school staff or administrators—Attackers pose as principals, superintendents or department heads to request sensitive information, approve financial transactions or prompt urgent actions. They may also research specific staff to personalize the fraudulent message. These attacks may use familiar language and spoofed addresses to appear legitimate.
- Fake IT or technical support emails with requests for password resets—These messages mimic trusted platforms or appear to come from internal IT staff, urging recipients to click on links to reset passwords or verify accounts. They often use urgent language that is designed to create pressure to act quickly without verification.
- Sending messages with malicious links or attachments—These communications may include PDFs, documents or files that contain malware or redirect users to fraudulent websites. They often appear to come from known contacts or trusted vendors, increasing the likelihood of being opened.
- QR code phishing—Cybercriminals may send emails or other electronic messages with embedded QR codes that lead to malicious sites. QR codes can bypass traditional link scanning tools, making them harder to detect and more likely to succeed.

NIS
National Insurance Services

- Phony job offers, prizes or grant opportunities—These schemes target staff or students with enticing but fraudulent offers. Victims may be asked to provide sensitive personal information or pay upfront fees, believing the opportunity is legitimate.
- Event-based scams—These exploit school events, health alerts, payroll updates or institutional closures to create urgency and lower suspicion. They rely on emotional triggers and time-sensitive messaging, prompting users to provide quick, uncritical responses that contain sensitive data.
- AI-generated phishing—These attacks use AI-created messages that are sophisticated and well-written, making them harder to detect due to their personalization and natural language. Attackers use AI to mimic familiar communication styles, increasing the odds that a target will reply with sensitive personal data.

The Consequences of Phishing Attacks

If a school falls victim to a phishing attack, significant consequences can result, including:

- Data breaches and identity theft—Phishing attacks can lead to unauthorized access to sensitive student, staff, and faculty data, including Social Security numbers, grades and financial and health records. This can result in identity theft and reputational damage.
- Financial loss—Schools may suffer direct financial losses through fraudulent transfers, payroll redirection or compromised payment processes. They may also be subject to fines, penalties and legal costs.
- Disruption of learning and operations—Successful phishing attacks can lead to system outages, locked accounts or ransomware infections that halt access to learning platforms and administrative systems. This can delay instruction, testing and communication, affecting both academic performance and institutional credibility.
- Loss of trust—Parents, students, personnel and the community may lose confidence in the institution's ability to protect sensitive information. This can impact enrollment, employee retention and community support.
- Legal and regulatory consequences—Various data protection laws may apply to educational institutions (e.g., the Family Educational Rights and Privacy Act, or FERPA, and state-specific laws), and a phishing-related breach may trigger violations, investigations, fines or mandatory notifications. Compliance failures can also lead to costly lawsuits.
- Increased IT and security expenses—After a cyberattack, schools often need to invest heavily in cybersecurity tools, staff training and incident response. These costs can divert funds from other areas and add strain to already tight budgets.

Training Teachers and Staff

To mitigate the risks of phishing attacks, school personnel should be regularly trained on ways to identify and report suspicious activity. These educational sessions should be interactive and engaging and include:

- Information on spotting signs and red flags of phishing messages—Personnel should be trained to recognize common indicators of phishing attempts, including:
    - An urgent tone or high-pressure language that demands immediate action (e.g., threats of account suspension or quick deadlines)
    - Misspellings and incorrect grammar that may be used throughout the communication
    - Unfamiliar sender addresses that subtly differ from legitimate ones
    - Generic greetings, such as "dear teacher" or "dear all staff" that do not specifically identify the recipient
    - Unsolicited requests for confidential information, including financial details, passwords or login credentials
    - Suspicious attachments or links, particularly those with vague descriptions or uncommon file types
- Learning about real-world phishing examples—These provide concrete, relatable examples of cybercrimes and demonstrate the impacts they can have.
- Simulated phishing tests—These allow personnel to practice identifying and reporting suspicious communications.
- Verification protocols—School personnel should be instructed on the proper procedures to confirm the legitimacy of requests (e.g., calling the sender to verify the message's authenticity) and domains (e.g., analyzing the domain name carefully) before responding to them or clicking on links.

Additionally, it is essential to provide ongoing updates and refresher training as cyber threats and cybercriminal tactics evolve. It is also crucial to ensure cybersecurity training is integrated into the new hire onboarding process and provided when faculty or staff switch roles within the institution.

Building a Phishing Resilient School Culture

Taking steps to establish a phishing-resilient school culture can strengthen cyber defenses and deter phishing attacks. Steps to consider include:

- Encourage transparent reporting. Create a safe environment where staff, faculty and students can report suspicious activity without fear of punishment. Clear reporting channels and regular reminders help facilitate this behavior.
- Foster collaboration between teachers, admin staff, and IT for early threat detection. Encourage regular communication between departments to identify and respond to cyber threats quickly. Shared responsibility can improve awareness and response time
- Leverage technology. Using technological solutions such as anti-phishing software that monitors and detects phishing attacks and multifactor authentication that requires a second step to access secure systems can strengthen an organization's cybersecurity posture.
- Incorporate student and parent/guardian training to further strengthen schoolwide cyber hygiene. Teach students and parents/guardians basic cybersecurity practices through engaging lessons and activities. Empowering them builds a stronger, more resilient digital culture.
- Implement regular system audits. Proactively identify vulnerabilities and ensure compliance by conducting routine audits and addressing any issues that are detected.
- Back up data. This can mitigate the effects of a phishing attack by ensuring the institution does not suffer total data loss following a breach.

Conclusion

Training teachers and staff to recognize and report phishing scams is a critical step in safeguarding school networks and protecting sensitive data. Schools can build a resilient frontline defense against evolving cyber threats, including phishing attacks by fostering awareness.

Contact us today for more risk management and insurance information.