PowerSchool

How to Build (and Fortify) a Human Firewall

Human error is the No. 1 factor of K-12 cyberattacks. That's why students, staff, and parents must learn and follow best practices and report data breaches or suspicious activity. **The more people understand their role in data security, the stronger the firewall.**

Recognize the Threats

A solid firewall starts with a foundation of education. Everyone needs to know common, new, and evolving cybersecurity threats and how to prevent them. Understand types and examples of phishing and ransomware attacks, malware, IoT risks, student hacks, and DoS attacks.

IN PRACTICE

- Provide **updated lists** of all types of attacks
- Give **tips and best practices** and continuously train
- Put your users to the test to **practice extreme vigilance**

Protect Passwords

Passwords act as keys to a safe box (holding your critical data). By using simple password management best practices, you can reduce an attacker's ability to access servers, systems, and network devices, which are prime targets.

IN PRACTICE

- **Use unique**, complex, alphanumeric **passwords**
- Avoid real or personal words or the **same ones across systems**
- Enable **multifactor authentication** (MFA)

Train for Phishing

Phishing attacks are where cracks in your human firewall most often occur. Ongoing training and testing can make sure users aren't tricked by even the most convinving malicious emails. Always know who you're dealing with.

IN PRACTICE

- **Educate users** with age-appropriate examples of attacks
- **Ensure encryption is used;** use web filtering to block phishing sites
- **Test users** with simulated phishing attacks

Vet Your Vendors

Your edtech vendors should strengthen your human firewall, helping protect data through technology safeguards, best practices, and dedicated staff. Make sure all your software and systems comply with all common security standards.

IN PRACTICE

- **Stick to strict criteria** when selecting vendors
- **Confirm security protections** and best practices are followed by vendors
- **Set guidelines** for what software staff can use

Report Suspicious Activity

A durable firewall isn't impenetrable, and cybersecurity incidents can happen. But reporting suspicious activity right away gives system administrators the chance to respond quickly to minimize damage.

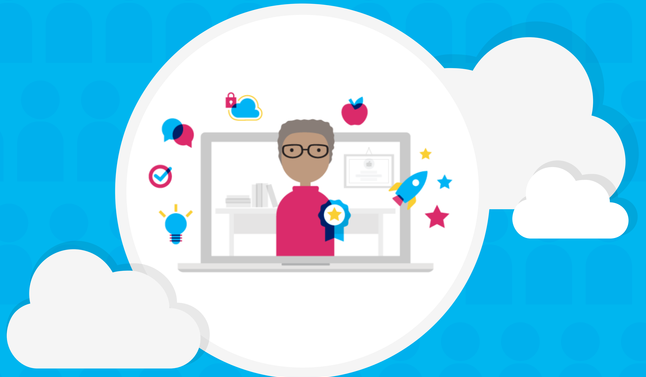
IN PRACTICE

- **Know who to contact** when there's an incident
- **Practice protocol** steps for reporting
- **Communicate** new and emerging threats that users should report

Take a Deeper Dive on Training Tips

Learn how a well-informed staff is your strongest ally in the fight against cybersecurity attacks.

BOLSTER YOUR FIREWALL



PS-TL-if-001-120820