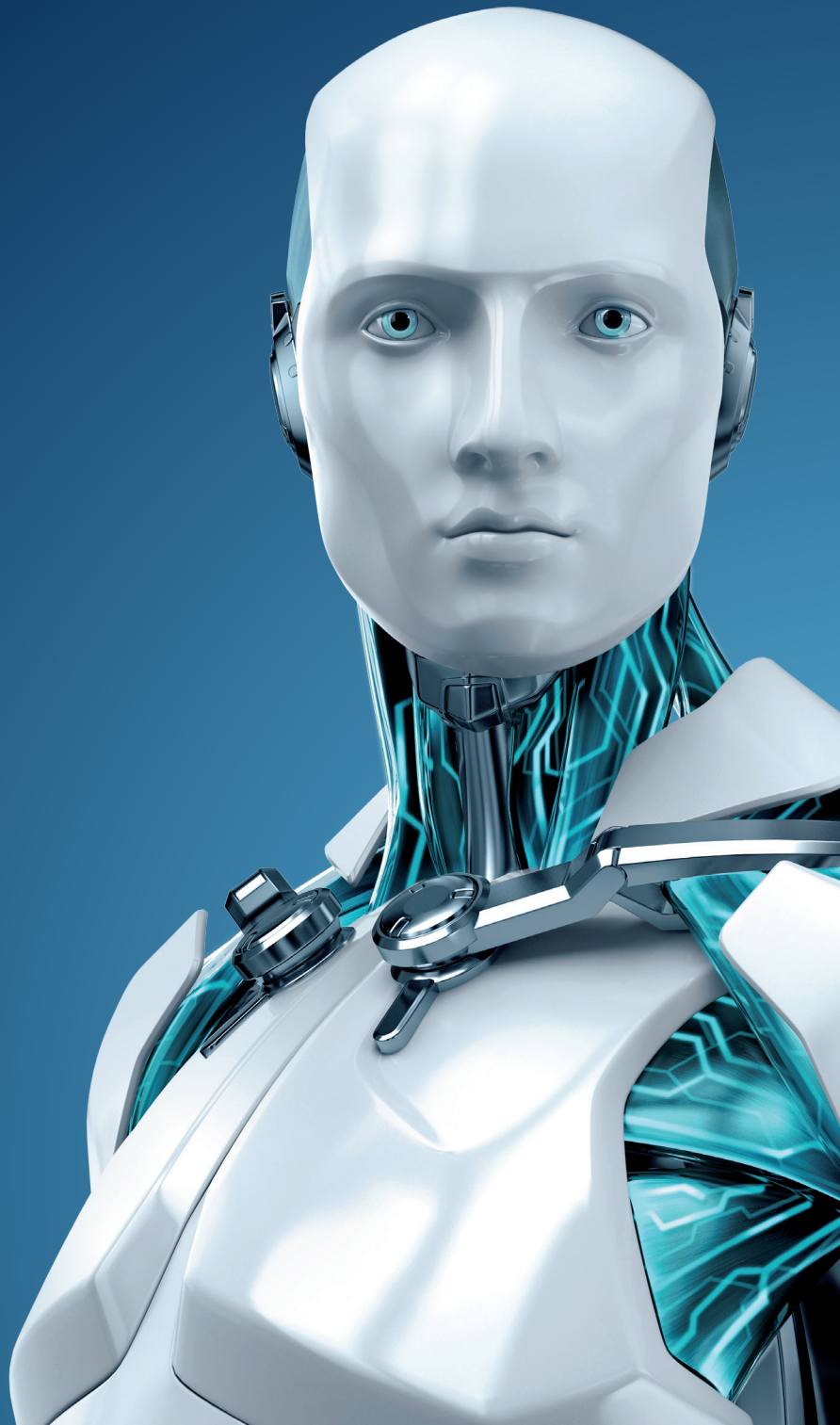
TECH BRIEF

Protection from cyber crime: Top 10 security measures for educational institutions



ENJOY SAFER TECHNOLOGY®

PROTECTION FROM CYBER CRIME: TOP 10 SECURITY MEASURES FOR EDUCATIONAL INSTITUTIONS

By Bruce Burrell, ESET Security Researcher

Every educational institution should be aware that cyber criminals make money by stealing personal information and selling it on the black market to other criminals, who then turn the data into cash through a range of fraudulent schemes.

Why do school administrators and educators need to know this? Because schools of all kinds—from primary through secondary and higher education—now have databases full of personal information about faculty, staff, and students. To cyber criminals, these repositories of personal data are a most appealing target.

A quick refresher on the scope of this problem.

- On February 18, 2014, the University of Maryland was the victim of a computer security attack that exposed records containing personally identifiable information (PII).
- A week later, Indiana University announced that a staff error had exposed information on 146,000 students for 11 months. And a week after that, the North Dakota University System reported that a server containing names and Social Security numbers for more than 290,000 current and former students and about 780 faculty and staff had been hacked.

Clearly, school networks are under attack, which means you can no longer act surprised if the bad guys come after the data in your systems. There's a thriving underground market for stolen credentials, from credit and debit cards to VPN access. Here are the 10 defensive measures you need to know and implement:

1. Layered defenses

Don't expect one security product alone will protect you against every possible threat to your systems and data. Of course, you should have an antimalware suite on all parts of your network (don't forget smartphones, Android™ tablets, Linux™ servers, and Mac® computers along with your Windows® machines). But you should also have a firewall at the gateway to your school's network and on all your individual machines–those you own, those owned by grants, and those owned by your students, faculty, and staff. Any important data, such as grades, finances, or personal information, should be encrypted both in storage (both on servers and workstations) and any time data leaves your machines, like via email or on devices like smartphones or USB sticks.

A solution like ESET Endpoint Security delivers multi-layered, cross-platform protection for Windows, Mac and Linux, along with firewall protection to minimize ID theft and Web filtering to block malicious sites. This versatile endpoint solution can be managed from a single console using the included ESET Remote Administrator. Adding DESlock+ Encryption enables you to encrypt valuable data both at rest and in transit, preventing unauthorized access and meeting compliance regulations.

2. Implement the principle of least privilege

This simply means that no person, machine, or system should have access to things they don't strictly need. For instance: student financial data should be in a different part of the network than

student health data. Both should be off limits to anyone who doesn't need to access it. Very few people, if any, should have administrator-level access rights on their own machines—and if they must have admin rights, they shouldn't be using that account except when they need to do admin tasks. Any time you can restrict access without disrupting people's ability to do their jobs, you should. Remember: the compromise of Target's point of sale terminals was executed via a supplier who had been granted access to some of the retail giant's computers.

3. Update, update, update

Applying updates and patches for all software is one of the most important things you can do to minimize the vulnerabilities criminals can use to silently get into your machines. When managing complex systems there may be a case for testing updates before rolling them out, but keep delays due to this process to a minimum. The bad guys are constantly probing for unpatched vulnerabilities. And don't forget that it's not just your operating systems and applications you need to keep patched; there are the helper apps that your browsers run, from Java to Flash to Acrobat and beyond.

4. Passwords are not enough

If you're protecting lots of personally identifiable data, a password alone may not be enough. Consider implementing two-factor authentication (2FA). This can be a biometric, like a fingerprint, or a one-time passcode that is provided to users via a small digital key card or fob.

A more recent development is the use of smartphones to deliver one-time passcodes to users and these systems can be relatively inexpensive yet highly secure. ESET Secure Authentication uses this technique to add an extra layer of protection against unauthorized access in case a device is lost or stolen.

5. Make sure all faculty, students and staff are picking good passwords

Despite one-time passcodes and other authentication developments like biometrics, passwords are likely be with us for a while, so make sure everyone knows how to make them hacker-resistant. A good password is unique, strong, memorable to the user, but hard for others to guess. That means it should be long, maybe even a phrase rather than a word or two. It should contain lower- and upper-case letters, numbers and special characters. Most important: each site or service that requires a password should have a different password.

6. Ban the sharing of credentials

Schools, colleges, and universities are often friendly places where people work together closely, so it may seem natural for folks to share usernames and passwords with colleagues or leave their machines open and logged onto the network in their own names. Unfortunately this behavior can undermine one of the best weapons we have for securing systems: log analysis. If the events recorded in the logs cannot be reliably attributed to the person who executed them, it is going to be hard to find out what happened when something goes wrong. Just as you should run a password cracker on the network logins from time to time to make sure nobody is using things like "qwerty" or "87654321", you should spot-check to make sure that when "jondoe" logs into fileserver3, it really is Jon!

7. Encrypt everywhere

We covered this a little in the "layered defenses" tip, but it very much bears repeating. When we have something that is valuable, we lock it up when it's not in use. It's the same with data, which should be encrypted whenever not directly in use. This minimizes criminals' ability to get any useful data, even if they do manage to breach your other defenses.

DESlock+ Secure Encryption allows administrators to efficiently deliver email, file, removable media and full disk encryption to Windows machines across networks and/or the Internet through an included cloud-hosted server, while DESlock+ Mobile for iOS enables encryption for iPhone and iPad.

8. Backup, backup, backup

Backups of your data and systems are the last, best line of defense against destructive criminal hackers. In the case of threats like data ransoming they may be the only way to beat the bad guys. You might consider backing up to the cloud, but do this as a compliment to, not replacement for, local backups that are both tested and stored securely.

Your best bet is a solution such as StorageCraft, a proven data backup and recovery system that promotes business continuity in case of security breaches or natural disasters.

9. Security training and awareness

As an educational institution, you should be aware that providing security training and awareness for employees and students is a must, and that it actually can be very successful as a protection mechanism. You can't expect people to abide by security procedures unless you explain how they work and why they are needed. Take advantage of the interactive, online cybersecurity training included with most ESET security products. You can also contact ESET to request additional onsite instruction for your staff.

10. Make a clean break

When employees leave and students move on, be sure to adjust their credentials accordingly. In many cases this will mean terminating their access to school systems. The use of lingering credentials that should have been revoked is one of the most common forms of "insider" abuse of systems. If faculty, staff or students depart abruptly and not on good terms, terminating all of their access immediately is a must. In addition, a review of authorized user accounts should be done at least once a year to weed out access that is no longer appropriate.

Of course, there's more that schools can do to defend their systems, but these 10 measures will serve you well and, when used together, can defeat many attackers.