IDENTIV WHITE PAPER

Verifying Identities in the Shifting EdTech Landscape

How Identiv Prevents Cyberattacks and Powers Passwordless, Platform-Agnostic E-Learning

Introduction

Education is evolving. While the virtual classroom, alongside education technology (EdTech) tools and practices aimed at enhancing learning, is not a new model in the university setting, K-12 institutions face daily challenges to verify access while safely and securely shifting to 100% virtual and hybrid learning environments. The reality is virtual and hybrid education is here to stay and the rapid surge in online learning affects all age groups.

According to the World Economic Forum (WEF), by the end of 2020, almost 1.4 billion children were home-schooled. While some universities already had distant learning digital strategies in place, the pandemic is shaping the future of higher education and pushing universities online.

The shift to online education means security concerns are at an all-time high. When it comes to security in the education space, a 2020 Malwarebytes report stated that educational institutions must brace themselves for a continuing onslaught of cyberattacks.

This paper highlights the importance of digital responsibility to ensure virtual learning is a safe experience for students as well as educators. It also discusses some common cyberattacks and their solutions so schools can create secure EdTech environments.

The Demand for Digital Responsibility as an Emerging Trend

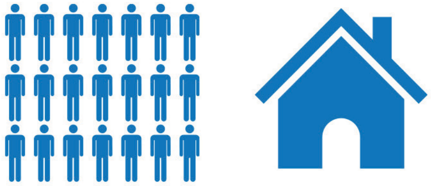
With online learning taking the forefront, parents want schools to help students develop healthy relationships with technology. Digital responsibility refers to ensuring that students are safe and confident explorers of the digital world.

The demand for digital responsibility is an emerging trend in EdTech, making good "digital hygiene" an essential practice in the virtual classroom and through other e-learning applications. Today, we are compelled to adopt new technologies in our everyday lives. We are thinking about the health of our devices, which are already a significant extension of ourselves.

Digital hygiene is our critical first line of defense against new and emerging digital threats, including malicious emails, social engineering, phishing, cyber harassment, hacking accounts, and devices, pilfering private data, or even worse.

1.4 BILLION

CHILDREN HOMESCHOOLED
BY THE END OF 2020



Cyberattacks Targeting K-12 Education Are on the Rise

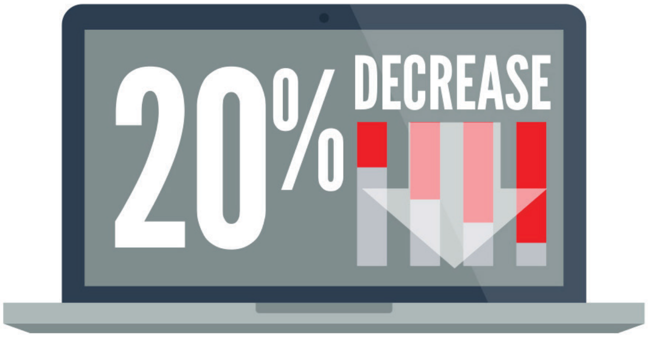
A look at the education sector's security landscape provides a tale of insecurities, cyber-incidents, and high financial stakes.

The K-12 Incident Map, a resource that records cyberattacks on K-12 education establishments, recorded 1,099 incidents since 2016. Attacks include unauthorized disclosures, breaches, or hacks that resulted in exposed personal data, ransomware, phishing, and Denial-of-Service attacks (DoS).

According to a report from the U.S. Government Accountability Office (GAO), thousands of K-12 students had their personal information compromised in data breaches between 2016 and 2020.

The 15th Ponemon Institute's Cost of a Data Breach Report on data exposure and other cyber-incidents looks at the cost of a data breach in the education sector. The report found that:

- **The average total cost of a data breach at an education establishment is $3.9 million.**
- **Malicious attacks caused 48% of cyberattacks in the education sector while system glitches and human error were the cause of the remainder.**
- **Only 18% of educational institutes in the U.S. use automated security, whereas the global average is 21%.**
- **It takes, on average, 212 days to identify and address a data breach that happens within an educational setting.**



in the cost of a cyberattack in 2020 compared to 2019

On the brighter side, the education sector's response, including better security measures such as strong authentication, is aiding a downward trend for these numbers. The education sector saw roughly a 20% decrease in the cost of an attack in 2020 compared to 2019.

However, the move to online education has severe ramifications for security. An FBI report in December 2020 warned of cybercriminal attacks against K-12 distance learning education stating:

"*As of December 2020, the FBI, CISA, and MS-ISAC continue to receive reports from K-12 educational institutions about the disruption of distance learning efforts by cyber actors.*"

To maintain a continued reduction in costs to the sector and ensure student and staff data security, education providers must understand the common cyberattacks to come up with suitable preventive measures.

Types of Cyberattacks

Here are some typical cyberattack types observed in online education settings:

1. Zoombombing

Zoom, Microsoft Teams, and other video conferencing platforms emerged as staggering success stories of the COVID-19 pandemic. EdTech platforms have felt their versions of the phenomena known as "Zoombombing", which became prevalent in 2020, as the Zoom platform reached massive uptake.

Remote classrooms and e-learning applications are not exempt from Zoombombing, including racist and sexist attacks and outright lesson hijacking. An FBI report in March 2020 warned of online lesson hijacking. Another report from Education Week describes how New Hampshire's Concord High School suffered several incidents, including pornographic images posted during online lessons.

How to Protect Against Zoombombing

Preventing Zoombombing is vital to ensure uninterrupted lessons and protect children from obscene, frightening, or offensive incidents. Countermeasures must include security hygiene practices:

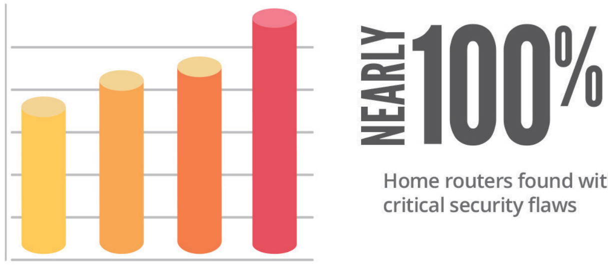
- **Use the meeting room feature or protect access using robust authentication. Secure access and authentication measures ensure that only legitimate students can enter.**
- **Use private lessons with unique private URLs.**
- **Any messages sent using the platform should be private or sent to selected members unless otherwise allowed.**
- **Control screen sharing and audio access.**

2. Home Security Issues

Virtual classroom and e-learning tools have the same security considerations as work-from-home or remote working. The Home Router Security Report 2020 found critical security flaws in almost all home routers. Some routers had hundreds of vulnerabilities.

A compromised router can even spy on you as a router under an attacker's control can stage a man-in-the-middle (MitM) attack. It can alter unencrypted data or send the user to "evil twin" websites masked as frequently used webmail or online banking portals.

Many consumer-grade home-gateway devices fail to alert users if and when firmware updates become available, even though those updates are indispensable to patch security holes. Some other devices will not accept passwords longer than 16 characters.



How to Protect Against Home Security Issues

The first step toward home security is to ensure the router and cable modem are not a single device. Consider buying a low-end commercial-grade router that is unlikely to have UPnP or WPS enabled. It also offers additional features, such as firmware rollbacks in case a firmware update goes wrong.

Some other quick fixes include:

- Change the administrative credentials from the default username and password.
- Make the password long, strong, and unique.
- Change the network name, or SSID, from default to something unique, but do not give it a name that identifies you.
- Turn on automatic firmware updates if they are available.
- Enable WPA2 wireless encryption so that only authorized users can hop on your network.
- Enable the new WPA3 encryption standard if the router supports it.
- If you have a lot of smart-home or Internet of Things (IoT) devices, connect them to your guest Wi-Fi network instead of your primary network.

3. Shared Devices and Device Theft

Often siblings share devices or parents share their devices with their children, allowing them to use computers and tablets to browse the internet in their spare time. These shared devices expose device-borne data, which is a major security concern. Shared devices can also be lost or stolen, allowing further exposure to the data and e-learning app access.

How to Protect Against Shared Devices and Device Theft

Here are a few tips to keep the devices that multiple people use as secure as possible:

- Each user must access a device using a secure authentication key based on the FIDO standard.
- For devices used in online learning, the platform must have robust authentication to control access to lessons. This makes lessons personalized and protects associated data.
- Delete auto-fill details. Otherwise, logging out of your account will not be enough to protect your private details.

4. Phishing

In 2020, we saw many phishing campaigns that used the pandemic and associated themes to target students and educators working remotely. One such campaign was ACH payment remittance phishing messages. An Education Week survey found that half of K-12 CTOs said phishing scams were a “significant or very significant problem”.

How to Protect Against Phishing

Here are a few simple steps to identify and prevent phishing scams:

- Apply robust authentication (such as two-factor) that stops a phishing attack even if a student or staff member clicks on a phishing link and enters a password.
- Avoid clicking on a link in an email or instant message, even if you know the sender.
- Download add-ons that detect a malicious website or alert you about known phishing sites.
- If the site URL doesn’t start with “https”, or you cannot see a closed padlock icon next to the URL, don’t enter any sensitive information or download files from that site.
- Regularly rotate your passwords so that you stop an attacker from gaining unlimited access.

5. Third-Party Software Risks

When learning online, you have to rely on cloud platforms and third-party software. Cybercriminals launch attacks on platforms with the intent of making those inaccessible or extremely slow. Attacks such as DDoS and ransomware are common against online learning platforms used by K-12 students.

How to Protect Against Third-Party Software Risks

While it is not possible to completely avoid third-party software, here is what you can do to mitigate the security risks:

- Occasionally review third-party service level agreements (SLAs) and non-disclosure agreements (NDAs).
- Educational institutions should set up business continuity plans to minimize service interruptions if

UNAUTHORIZED DISCLOSURES, BREACHES, AND HACKS

Result in exposed personal data, ransomware, phishing, and Denial-of-Service attacks (DDoS)

the worst happens. This includes upgrade and patch management plans and security policies.

- **Keep operating systems updated to prevent cyberattacks. It can also lead to enhanced capability.**
- **Create an open channel for communicating threats and risks to the third party.**

Standards and Regulations Related to EdTech Security

Cybersecurity concerns may focus on ensuring that students have uninterrupted learning when using a virtual classroom environment or EdTech application. However, educational establishments also have to contend with the needs of data protection and privacy regulations. Two of these regulations and standards include:

Children's Internet Protection Act (CIPA)

Introduced in 2000, CIPA is enforced by the Federal Communications Commission (FCC). It specifically addresses the concerns on children's access to obscene or harmful content over the internet. To accommodate the requirements of CIPA, an educational establishment must use tools, such as internet filters and robust authentication, to protect children against harmful content like pornographic images posted by Zoombombers.

CIPA specifies several areas that education centers must cover using policies and technical measures including:

- **Restricting minors' access to inappropriate content**
- **Safe use of email and messaging**
- **Limiting unauthorized access and unauthorized disclosure of personal information**

Educational establishments must monitor students' activities when online and provide training to protect them against harmful people and elements found in an online context.

Adhering to CIPA requires a layered security approach, starting with robust authentication and access control. It also includes measures such as secure email gateways, anti-phishing measures, and endpoint protection.

Children's Online Privacy Protection Act (COPPA)

COPPA imposes certain requirements on website operators or online services directed to children under 13 years of age, and on administrators of other websites or online services that are collecting personal information online from a child under 13 years of age. It also gives parents control over what information websites can collect from their children.

Website operators covered by the Act must:

- **Post a clear online privacy policy describing their practices for personal information collected online from children**
- **Provide direct notice to parents and acquire verifiable parental consent**
- **Provide parents access to their child's personal information to review and/or have the information deleted**
- **Maintain the confidentiality, security, and integrity of information they collect from children**

Key Solutions to Prevent Cyber Threats in EdTech Platforms

The threats experienced during the surge in online learning have thrown educators a security curveball. The types and levels of cyber threats focusing on online education platforms and e-learning tools have made EdTech a battleground. The education sector must find solutions to these threats to ensure that education across all age groups is seamless, secure, safe, and continues unabated.

Here are a few technology solutions that can help educators and parents ensure a safe online learning experience for students:

Two-Factor/Multi-Factor Authentication

A much-touted robust authentication method is the use of two or more factors. For example, a password PLUS another form of authentication, such as an SMS text message containing a PIN. However, there are a few challenges with this type of multi-factor (MFA) authentication:

- **The method requires users to remember a password.**
- **It can be costly if using SMS texts.**

- **If using a second-factor app, the user has to download and install the app, and if the phone is lost or stolen this can cause problems with legitimate access.**

uTrust FIDO2 NFC Security Keys

Made in the U.S., Identiv's uTrust FIDO2 NFC Security Keys take multi-factor authentication one step further. They provide a simple, strong authentication experience that eliminates the need for passwords.

Based on free, open standards from the FIDO Alliance, Fast IDentity Online (FIDO) authentication replaces password-only logins with safe, fast login experiences across websites and apps. This is possible by using standard public-key cryptography to provide strong authentication and leave zero data at rest. FIDO U2F is an open standard that provides additional security and streamlines Universal 2-Factor authentication.

With a balance between usability and security, Identiv's uTrust FIDO2 NFC Security Keys allow individuals, schools, and other organizations to replace passwords with a secure, fast, scalable, cost-effective login solution. This way, it helps by:

- **Reducing the need to remember and type passwords**
- **Working with everyday devices, including phones, tablets, laptops, and desktops**
- **Allowing one device to work across all services (such as G Suite for Education, Gmail, Microsoft Office 365, YouTube, Dropbox, etc.)**

uTrust FIDO2 Security Keys support both contact (USB A/C) and contactless (NFC) use-cases. The solution provides multi-protocol FIDO U2F, FIDO2, smart card, and OTP support, and is compatible with Windows, Linux, macOS, Android, and iOS.

Identiv's security keys based on FIDO standards mitigate many cyber threats. They help stop phishing, control access to sensitive data, and prevent nefarious individuals from accessing students' e-learning environments. As a result, you can achieve a secure virtual classroom by using a user-friendly form of authentication.

Conclusion

Regardless of the EdTech platform, the most effective way to ensure e-learning security is to stop attacks at the entrance point, i.e., via access control. Robust authentication measures verify identities and maintain a secure online experience for students and make the most of online learning.

Open standards, like FIDO, are the basis for a safe online learning environment. But these measures must take users into account, and the device must be usable and cost-effective. Ultimately, the authentication type chosen to secure the e-learning environment should be an end-to-end security and access control solution that ties into existing infrastructures without causing disruption.

The online learning experience may continue to evolve for today's students, but we cannot allow cybercriminals to obstruct continued excellence in education. Exceptional authentication measures like Identiv's uTrust FIDO2 Security Keys can provide the required environment to maintain seamless education.

For more information on Identiv's EdTech security products and solutions, call +1 888.809.8880, contact sales@identiv.com, or book a demo.

Identiv, Inc. (NASDAQ: INVE) is a global leader in digitally securing the physical world. Identiv's platform encompasses RFID and NFC, cybersecurity, and the full spectrum of physical access, video, and audio security. For more information, visit **identiv.com** or email **sales@identiv.com.**

© Identiv, Inc. | All rights reserved. This document is Identiv public information.