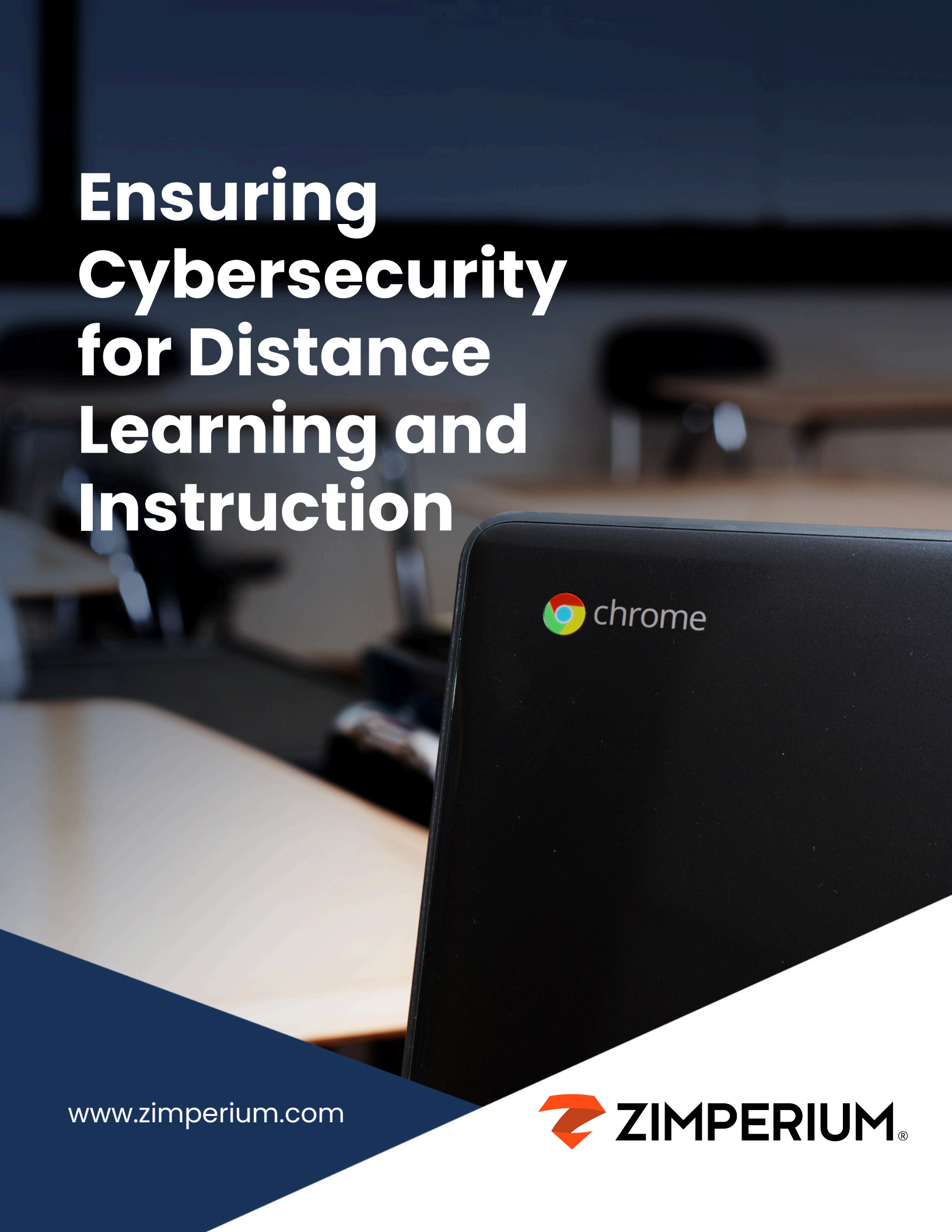
Ensuring Cybersecurity for Distance Learning and Instruction



www.zimperium.com

ZIMPERIUM®

Ensuring Cybersecurity for Distance Learning and Instruction

Virtual learning and remote instruction are foundational to enabling K-12 schools to perform their educational mission in a post-pandemic society. Funding for the technologies making distance learning possible, and the modernization of existing school technology infrastructures required to support it, was part of the $2 trillion Congressional stimulus package known as the CARES Act.

In addition to the $13.2 billion for K-12 schools in the CARES Act, funding for education has been part of the various subsequent acts under consideration by the Congress.

K-12 school districts have broad discretion in the use of funds they receive from the CARES Act, and the acquisition of distance-learning-enabling educational technology, including hardware, software, and connectivity, is among the specified uses.

Some of that technology may be relatively new to students and educators, making it particularly important to protect endpoint devices, such as Chromebooks, that are provided for use outside of the school's firewalls. These devices are vulnerable to attacks that could not only compromise the user's security and privacy, but also provide a pathway for bad actors to further attack the school's network.

> "The CARES Act includes a long list of allowable activities, including... **support for education technology essential to distance learning"**
>
> **Wallace Foundation**
> https://www.wallacefoundation.org/news-and-media/blog/pages/the-cares-act.aspx

> "As individuals continue the transition to online lessons and meetings, the FBI recommends exercising due diligence and caution in your cybersecurity efforts."
>
> **FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic**
>
> https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

Although cyberattacks against educational institutions have been ongoing for some time, we've seen increases since the start of the pandemic. To cite just a few examples:

- The Rialto Unified School District in California suffered a malware attack and had to close virtual classrooms for a week.
- The Miami-Dade County Public School system was subjected to a distributed denial of service (DDOS) attack that left students struggling to access their online classrooms.
- The Haywood County School district in North Carolina was the target of a ransomware attack that shut students out and left some services unavailable for weeks.

Cybersecurity in Distance Learning

Chromebooks are widely recognized as an effective technology for enabling remote education. However, the use of Chromebooks in distance learning creates a level of cybersecurity risk.

Students, teachers, and administrators using Chromebooks face the same privacy and security threats associated with laptops and mobile devices, but without the same security measures. This is because many protective solutions widely available for use on traditional devices are not available for Chromebooks.

As a result, Chromebooks are vulnerable to threats such as:

- **Bad Wi-Fi** - Loss of personal information, including grades and health data
- **Phishing** - Stolen credentials could be used to steal money or evencompromise social media accounts
- **Malicious Apps** - Spyware and other malicious apps could expose data or deliver a device exploit
- **OS Exploit** - Cameras and microphones can be turned on, anytime day or night
- **Risky Apps** - Private information can be shared without any user knowledge or consent

Protecting Remote Learning Devices Against Cyberthreats

The complexity of providing cybersecurity remotely is exacerbated by factors such as inconsistent or limited bandwidth and connectivity. If a cybersecurity solution for a device such as a Chromebook requires uninterrupted cloud connectivity, intermittent access will render the solution ineffective. The solution must therefore operate entirely on-device and have no requirement for internet connectivity.

The only comprehensive, on-device, machine learning-based security solution for Chromebooks is Zimperium MTD for Chromebooks. MTD for Chromebooks:

- Assesses all Android apps for malicious intents/capabilities, undesired violations of privacy or unsecure development practices;
- Detects malicious Wi-Fi networks and alerts users to disconnect from the network;
- Identifies and blocks users from accessing phishing sites; and
- Protects user privacy while providing IT administrators with centralized visibility into any attacks so they can take quick action.

In this way, MTD for Chromebooks helps educational institutions reduce their risk by detecting the most advanced device, network, phishing, and malicious app attacks.

Deriving Long-term Value

Distance learning appears to be a long-term strategy for some schools. The cybersecurity risks associated with remote learning will continue to grow and evolve. Investments in cybersecurity today will therefore solve immediate problems and will also continue to provide value over time.

If you'd like to learn more about Zimperium cybersecurity solutions for distance learning, please don't hesitate to contact us. We look forward to speaking with you.

https://www.zimperium.com/contact-us/

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244