GoSecure

USE CASE BROCHURE

EDUCATION

CYBER ATTACKS ARE ON THE RISE, AND A GROWING NUMBER OF SCHOOLS ARE IMPACTED BY IT

PHISHING IMPACT IN NUMBERS

29%

Of attacks on educational institutions originated from vulnerability exploitation and 30% from phishing campaigns on K-12 schools in 2023.

$53 BILLION

Ransomware attacks on K-12 and higher education globally caused over $53 billion in downtime costs from 2018 to mid-September 2023.

6.7 MILLION

These attacks breached over 6.7 million personal records across 561 incidents.

Your ally to consolidate, evolve & thrive

PHISHING ATTACKS RELY ON HUMAN ERROR

Statistics suggest that while many educators and staff typically follow email hygiene and safe usage guidelines, there is always a small number who may forget or overlook these critical practices.

One wrong click on a suspicious email by someone in your school or district could unknowingly give cybercriminals access to your network and sensitive information.

With this unauthorized access, bad actors could steal student and staff data, disrupt teaching and administrative operations, or damage your institution's reputation.

Despite frequent IT security reminders to avoid clicking on unsolicited emails, hackers are counting on the likelihood that at least one person in your education community may trust an innocent-looking attachment or hyperlink.

HAZARDS FROM A COMPROMISED EMAIL INCLUDE:

- PHISHING ATTACKS
- BUSINESS EMAIL COMPROMISE
- ADVANCED MALWARE
- RANSOMWARE
- SOCIAL ENGINEERING THREATS
- BRAND FORGERY

Worse yet, users with elevated privileges could inadvertently give hackers the “keys to your kingdom”.

INFO@GOSECURE.AI

www.GOSECURE.AI

GoSecure

PROTECTING EDUCATION WITH GOSECURE

Through tailored solutions, a commitment to innovation, and a deep understanding of the education sector's unique challenges, GoSecure leads the way in safeguarding schools and institutions against cyber threats.

CHALLENGES

LACK OF DEDICATED IT RESOURCES

Many educational institutions, particularly K-12 schools, often have limited budgets for IT infrastructure and security. This leaves them vulnerable to cyberattacks due to outdated software, insufficient firewalls, or a lack of skilled personnel to handle security issues.

INCREASE IN PHISHING AND RANSOMWARE ATTACKS

Educational institutions are increasingly targeted by phishing scams and ransomware. Attackers see schools and universities as easy targets because of the high volume of digital communication and the often limited cybersecurity awareness among staff and students.

PROTECTION OF SENSITIVE DATA

Schools handle sensitive information, including personal data of students, staff, and parents. Ensuring that this data is securely stored and accessed only by authorized personnel is a constant challenge, particularly as systems grow more complex.

A GROWING NUMBER OF DEVICES AND USERS

With the rise of digital learning tools, students and staff are accessing school networks with multiple personal devices (e.g., laptops, tablets, smartphones). Managing and securing all these endpoints while preventing unauthorized access is a major challenge.

GOSECURE'S RESPONSE

GoSecure's advanced threat detection solutions can monitor school networks in real-time, identifying suspicious activity and neutralizing threats before they cause harm. This proactive approach helps schools manage cybersecurity threats even with limited internal resources.

GoSecure offers strong defenses against phishing and ransomware attacks. Their security solutions include email filtering and threat analysis to detect suspicious messages and links, helping to prevent staff and students from falling victim to these schemes.

GoSecure provides tools for encrypting sensitive data and managing access to ensure that only authorized users can access critical information. This helps safeguard student records, personal information, and other confidential data.

With more devices accessing school networks, GoSecure offers endpoint security solutions that help protect every device connected to the network. This reduces the risk of cyberattacks spreading through vulnerable or unprotected devices.

INFO@GOSECURE.AI

www.GOSECURE.AI

Your ally to consolidate, evolve & thrive

Your ally
to consolidate,
evolve & thrive

GOSECURE TITAN® MANAGED EXTENDED DETECTION & RESPONSE (MXDR)

DETECT & MITIGATE FASTER

GoSecure Titan® Managed Extended Detection & Response (MXDR) offers the best-in-class response time from threat detection to mitigate with a solution that identifies, blocks, & reports potential breaches.

With early warnings, GoSecure Titan® MXDR blocks many attacks before they can impact an organization, all while consolidating critical security data, providing unmatched visibility and delivering proven protection with customizable views. We work with teams to address evolving threats, changing technology and constraints.

WITH PHISHING ATTACKS ON THE RISE, EXPERTS ESTIMATE THAT NEARLY A THIRD OF USERS OPEN A PHISHING EMAIL AND MORE THAN 10% OF THOSE USERS WILL CLICK ON A LINK OR OPEN AN ATTACHMENT

Included in every GoSecure Titan® MXDR bundle, GoSecure Titan® Inbox Detection & Response (IDR) give users a faster, easier way to take the guesswork out of questionable messages. With the ever-present GoSecure Titan® IDR icon in the toolbar of the Outlook application, users are reminded of the support available for any message they find even a little suspicious.

Messages are reviewed through both machine learning filters and GoSecure's expert analysis so that users can be reassured the message is safe upon return —or that it will be removed if there is a threat.

When a message status is returned to the user within minutes, their security awareness is reinforced, and the organization is better protected against breaches. Plus, the in-house security team gets full visibility to the entire process without lifting a finger.

In 2023, GoSecure Titan® IDR handled 123,745 submitted emails. Of those submitted emails, 89,100 were deemed to be threats.

GoSecure Titan® IDR makes users part of the solution, while offering the support that in-house teams need to address the onslaught of email threats today. With easy submission from right inside the inbox, users get both automated scanning and professional human threat evaluation of questionable messages from the experienced team at GoSecure.

A FOUNDATION YOU CAN TRUST & BUILD UPON

GoSecure Titan® MXDR consolidates critical security data, provides unmatched visibility, and delivers proven protection with customizable views. We work with teams to address evolving sophisticated threats like ransomware and fileless attacks, changing technology and constrained resources.

LEARN MORE