KnowBe4

From Primary Schools to Universities, the Global Education Sector is Unprepared for Escalating Cyber Attacks

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | Email: Sales@KnowBe4.com

Some schools endure over 2,500 attempted cyberattacks a day, earning them the label “target rich, cyber poor” from the U.S. Cybersecurity and Infrastructure Security Agency (CISA).[1]

The second part of this nickname refers to how most educational institutions, especially public ones, lack the resources that many other sectors enjoy—namely, robust and comprehensive cybersecurity programs.

This is particularly concerning given that typical IT systems of primary schools hold personal information of very young children, including home addresses, health records, and even confidential mental health records. Higher education institutions hold the same kinds of records; but they may also host payment processing systems and networks that are used as internet service providers (ISPs) to offer personal email services, and valuable intellectual property that is often ripe for espionage.

1 “Cybersecurity for K-12 Education,” *US Cybersecurity and Infrastructure Security Agency (CISA)*, n.d., https://www.cisa.gov/K12Cybersecurity

The Inherent Vulnerabilities of the Education Sector

The trove of sensitive information stored on an educational institution's servers makes it a prime target for cybercriminals. And while they may not be the most lucrative victims, there are several factors that make intrusion and extortion for ransom easier than organizations or institutions in financially stronger and better-equipped sectors.

With the rapid growth of cloud services, mobile devices, and hybrid learning environments, educational institutions have had to manage increasingly complex identity and access controls. Additionally, the rising use of AI presents new challenges. Cyber attackers are now specifically targeting both on-premises and cloud-based AI systems and data that have not been fully secured, seeking to bypass ineffective security measures and gain unauthorized access.

Primary education: Vulnerabilities and risks

The emotional impact

The exposure of young students' personal information triggers an emotional response. The consequences, such as attracting predators or increasing the risk of online harassment, feel more severe than in cases involving adults.

Urgency and reputation

These factors escalate the urgency of a cyber incident or intrusion at a primary school, as well as the potential reputational damage to the institution if the information is exposed on the dark web. Cyber attackers leverage this heightened risk, as they appreciate these institutions are more likely to pay a ransom to prevent stolen data from being exposed.

Outdated IT systems

An attacker's search for an open door is helped by the fact that with limited resources, and increasing demands for modernization, schools and universities often mix modern and legacy IT systems, which can leave highly sensitive personal information on outdated and exploitable systems. Particularly in the United States, both students and faculty are more likely to use personal devices in education.

Higher education: Unique challenges and cybersecurity risks

Attractive targets

Higher education institutions face distinct challenges that make them attractive targets for cyber attackers. With complex networks and large amounts of sensitive data, high schools and universities are often vulnerable to intrusion and extortion.

Research and collaboration

The core of higher education—research and innovation—drives collaboration. This reliance on sharing sensitive data with others, whether across campuses or institutions, poses security risks. As reported by Microsoft, faculty and researchers often collaborate with people they haven't met and may unknowingly share sensitive topics. This increases the likelihood of sensitive data ending up on public file servers or storage systems.

Students' lack of security awareness

In higher education, students often use personal devices without training on security protocols, accessing institutional networks and email systems. They may also work from shared accommodations or connect to free public Wi-Fi, creating additional vulnerabilities.

Diverse campus ecosystems

Universities have a diverse ecosystem of staff, faculty, and students, all of whom interact with the institution's networks for various purposes. Employees in administration, health services, food services, and more use systems for everything from recording health information to managing open email systems. This diversity makes the environment highly fluid and vulnerable.

Remote learning and increased attack surface

With the growth of virtual and remote learning, universities have expanded their digital infrastructure. This broadens the attack surface, as more systems, devices, and networks are interconnected, increasing the risk of potential breaches.

Common factors: External risks and communication

Reliance on third-party vendors

Both primary and higher education institutions heavily rely on third-party vendors for software-as-a-service, cloud storage, and IT services. This creates a risk, as vulnerabilities or breaches within third-party systems could later affect all institutions using these services, which often goes on undetected.

Balancing security and open communication

In both primary and higher education, institutions face the challenge of balancing cybersecurity with the need for open communication and collaboration. While robust security systems are essential, closing off communication entirely would undermine the very essence of the educational process—sharing knowledge. Finding this balance is crucial in safeguarding against potential breaches.

The Rising Tide

From every angle, the number of attacks against educational institutions is soaring, and shows no signs of relenting.

The reported number of attacks varies across different studies. Some measure attempted attacks; others only successful attacks. Of those, some measure attacks that resulted in a data breach; others measure only those where ransoms were paid. But one thing is clear: the number of attacks on the global education sector has risen sharply and is extremely concerning. The rise in attacks has pushed the education sector into the top five most frequently targeted globally, with some reports placing it at the very top.

In their 2024 State of Ransomware in Education report, provider of anti-virus and anti-malware software Malwarebytes called 2023 "the worst ransomware year on record" for the education sector.[2] This included a staggering 105% increase in known ransomware attacks against K–12 and higher education, surging from 129 attacks in 2022 to 265 in 2023. In higher education specifically, the report noted that attacks were up 70% over 2022.

According to the report, 43% of all ransomware in education attacks in 2023 targeted higher education and 36% of attacks targeted K-12. Geographically, while the US clearly absorbed the bulk of the attacks, the report also noted that the UK also had "a huge target on their back."

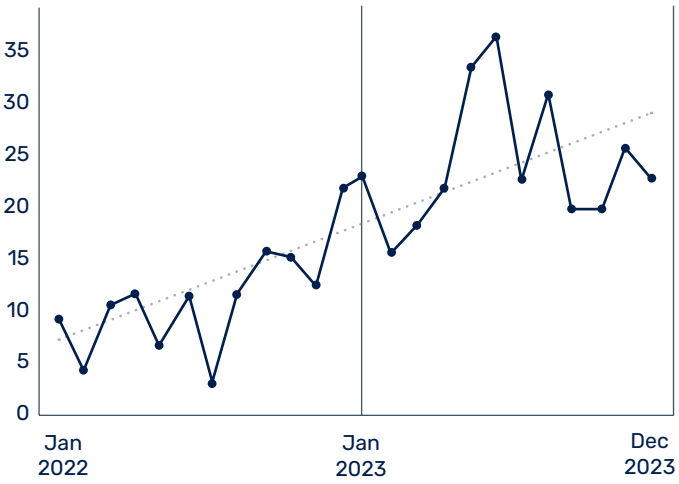


Fig.1 Ransomeware attacks on education

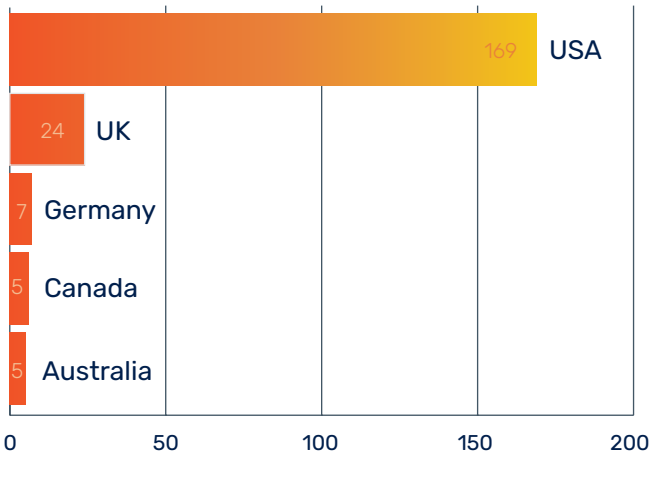


Fig.2 Geographical ransomeware attacks

2 Cozens, Bill, 2024 State of Ransomware in Education: 92% spike in K-12 attacks, Threat Down by Malwarebytes, January 24, 2024, https://www.threatdown.com/blog/2024-state-of-ransomware-in-education-92-spike-in-k-12-attacks/

In its 2024 Data Breach Investigation Report (DBIR), Verizon examined 30,458 security incidents in total, of which 10,626 were confirmed data breaches.

Of these, 1,780 incidents (17%) were attacks against the education system, 1,537 (14%) with confirmed data disclosure; a figure that put education in the top five of all industries breached globally. The DBIR noted that 98% of threat actors involved in the breaches were motivated by financial gain, while 2% were motivated by espionage. In addition, 83% of the data compromised in these breaches was personal information.

It didn't get better in 2024.

According to Check Point Research, the education sector was the industry most targeted for cyberattacks in 2024.[3] In its State of Cyber Security 2025 report, Check Point placed the average number of weekly cyberattacks on educational institutions at 3,574, a 75% increase from the previous year:[4]

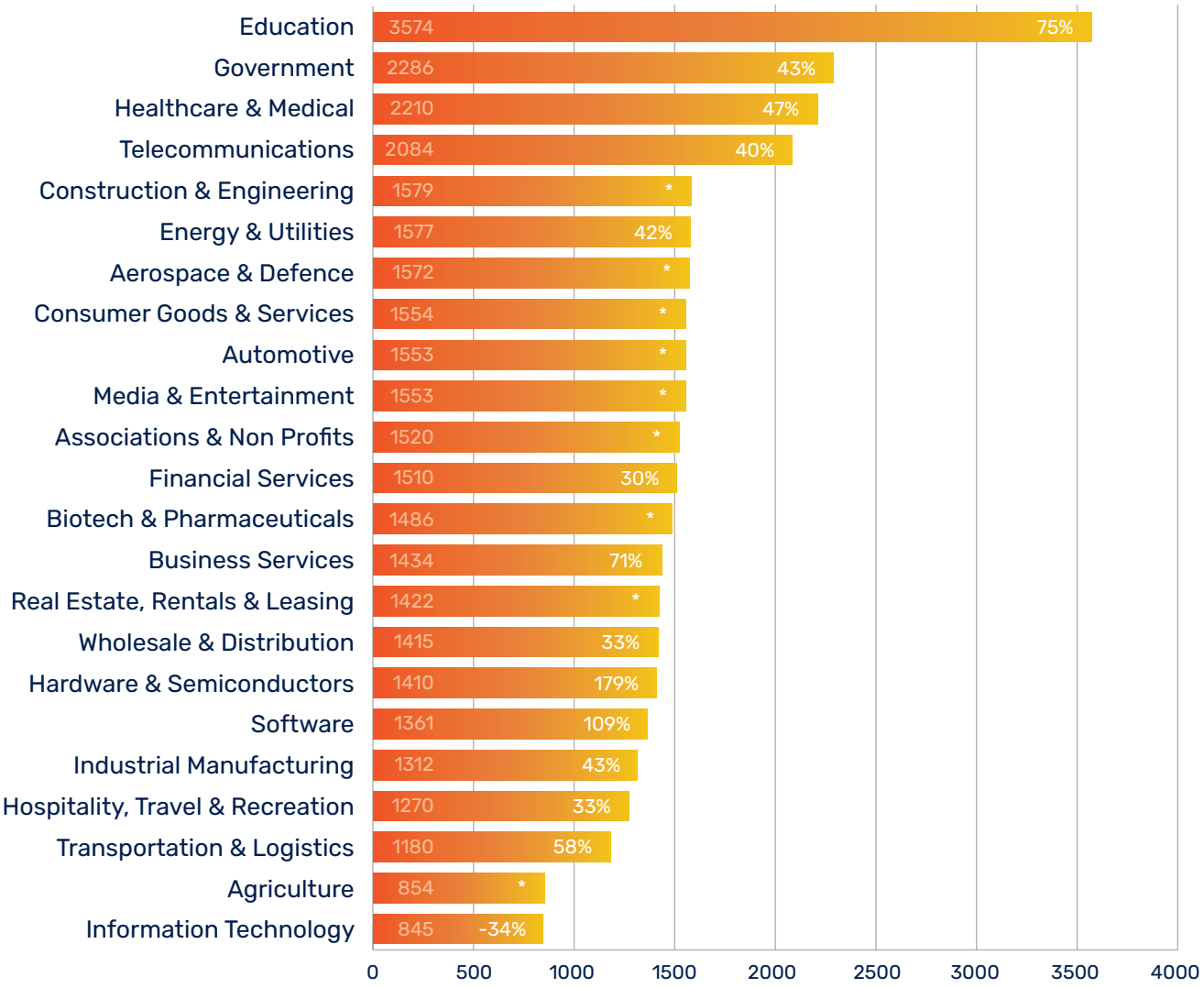


Fig.3 Global average of weekly attacks per organization by industry in 2024 (% of change from 2023).
(*) Newly introduced sectors which were not part of the previous report.

3 "Check Point Research Warns Every Day is a School Day for Cyber Criminals with the Education Sector as the Top Target in 2024", Check Point Team, August 13, 2024, https://blog.checkpoint.com/research/check-point-research-warns-every-day-is-a-school-day-for-cybercriminals-with-the-education-sector-as-the-top-target-in-2024/
4 "The State of Cybersecurity 2025," Check Point Research, January, 2025, https://www.checkpoint.com/security-report/

In its *October 2024 Cyber Signals* report, Microsoft Threat Intelligence marked education as the third most targeted sector of 2024, noting that over the past year, they had blocked more than 15,000 quishing (QR Code Phishing) emails per day to the education sector.[5] This figure only accounts for quishing, phishing attacks containing malicious QR codes, one of many tools in the hackers' arsenal.

Microsoft also identified the United States as facing the greatest threat activity, though other countries are also heavily impacted. According to the United Kingdom's Department of Science Innovation and Technology 2024 Cybersecurity Breaches Survey, 43% of higher education institutions in the UK reported experiencing a breach or cyberattack at least once a week.[6]

The largest attacks of 2024

>> Toronto District School Board data breach

In September 2024, it was reported that 2023/24 school year data had been compromised from Canada's largest school board district, which oversees 582 schools and 235,000 students. The attack, which was launched by the LockBit ransomware group, affected personal data including names, email addresses, student numbers, dates of birth, and more.

>> Highline Public Schools ransomware attack

On September 7, 2024, the Highline Public School district in Washington State was forced to shut down its K-12 schools and cancel all activities after the discovery of a ransomware attack. Highline has over 2,000 staff members and 17,500 students across 34 schools in the Burien, Des Moines, Normandy Park, SeaTac, and White Center communities in Washington State. All 34 schools were closed. They reopened a week later but it was mid-October before its systems were fully back online.

>> Mobile Guardian breach

In August 2024, a hacker breached Mobile Guardian, a digital classroom management platform used worldwide, and remotely wiped data from at least 13,000 students' iPads and Chromebooks. Mobile Guardian is a cross-platform (Android, Windows, iOS, ChromeOS, macOS) one-on-one solution for K-12 schools offering a suite of device management, parental monitoring and control, secure web filtering, classroom management, and communications. The breach impacted operations in North America, Europe, and Singapore.

>> Kansas State University cyberattack

On January 14, 2024, Kansas State University's network services were disrupted by a cyberattack, affecting the University's VPN, emails, Canvas videos, and Media site. The systems came back online January 25.

>> University of Winnipeg data theft

On March 25, 2024, weeks before exams were set to begin, the University of Winnipeg in Canada was hit by a cyberattack that shut down network access and forced class closures. The University confirmed on April 4 that personal information was stolen and exposed, including names, email addresses, social insurance numbers, and banking information of students enrolled in undergraduate and graduate programs since 2018, current and former employees of the university since 2003, and students who were issued T4A forms since 2016. The list was later expanded to include international students from 2014 to 2024, contractors who the university collected a social insurance number from, and people who provided personal health information relating to complaints and concerns over discrimination, harassment, sexual violence or a security incident from 2015 to 2024.

5 "Cyber Signals Issue 8 | Education under siege: How cybercriminals target our schools," Microsoft Threat Intelligence, October 10, 2024, https://www.microsoft.com/en-us/security/blog/2024/10/10/cyber-signals-issue-8-education-under-siege-how-cybercriminals-target-our-schools/

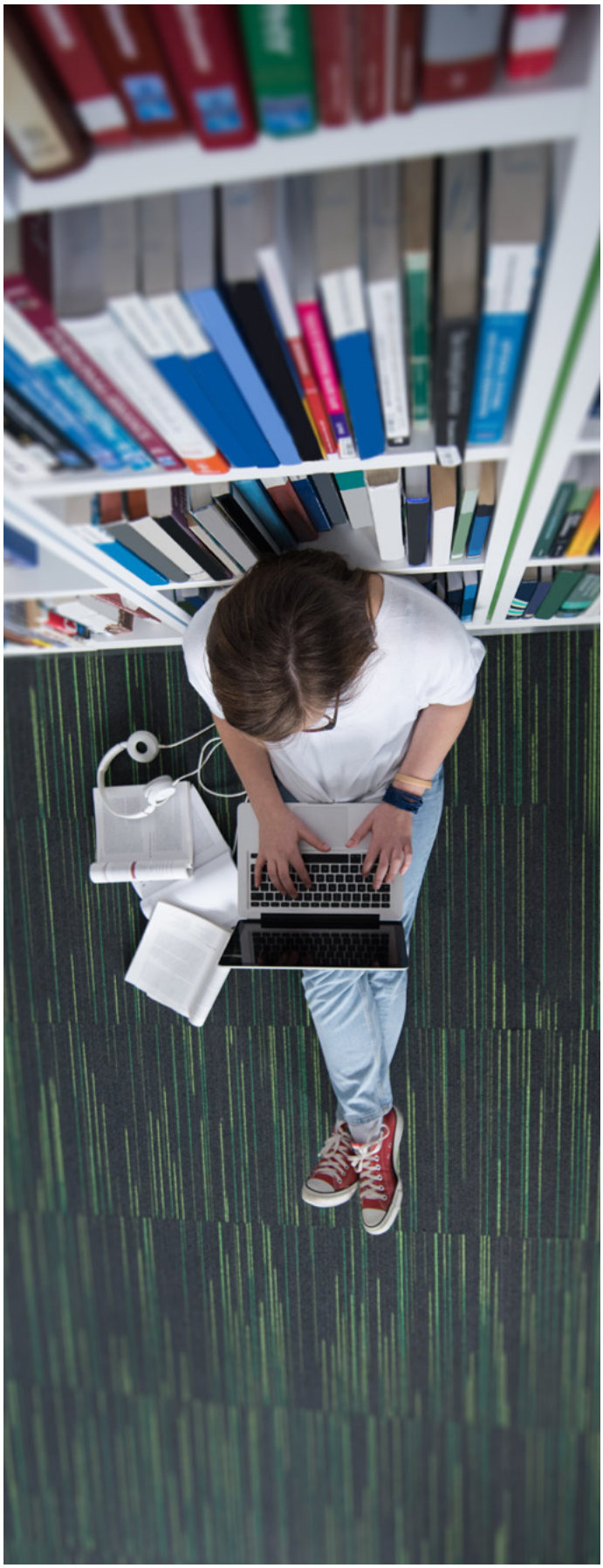
6 "Cyber security breaches survey 2024: education institutions annex," Home Office, Department for Science, Innovation & Technology, April 9, 2024, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024-education-institutions-annex

Nation states targeting higher education

It is not uncommon for universities to be partners on federally funded research, working with defense, technology, and other organizations in the private sector. This makes them centers of highly sensitive intellectual property. An attacker with their eye on this type of information will often find it easiest to penetrate through the more porous education institution; apart from providing valuable information themselves, the foothold can be used to springboard to higher value targets in government and industry.

Microsoft has observed two Iranian attack groups, Peach Sandstorm and Mint Sandstorm, launching social engineering attacks against targets in the education sector to gain access to infrastructure and research facilities.[7] Additionally, these groups use social engineering tactics to trick education sector targets into downloading malicious files, including a new, custom backdoor called MediaPI. According to the report, the Iranian Mabna Institute conducted intrusions into the computing systems of at least 144 United States universities and 176 universities in 21 other countries in 2023. The stolen login credentials were used for the benefit of Iran's Islamic Revolutionary Guard Corps and were also sold within Iran through the web. Stolen credentials belonging to university professors were used to directly access university library systems.

The same study notes that North Korean attack group Emerald Street has been targeting academics, primarily in Asia, for more than a decade. Another North Korean group, Moonstone Sleet, has been creating fake companies to forge business relationships with educational institutions or a particular faculty member or student. One of the most prominent attacks from Moonstone Sleet involved creating a fake tank-themed game used to target individuals at educational institutions, with a goal to deploy malware and exfiltrate data.



7 Cyber Signals Issue 8 | Education under siege: How cybercriminals target our schools, Microsoft Threat Intelligence, October 10, 2024, https://www.microsoft.com/en-us/security/blog/2024/10/10/cyber-signals-issue-8-education-under-siege-how-cybercriminals-target-our-schools/

The Attacker's Toolbox: Ransomware and Phishing

Ransomware attacks are easily the most prominent form of attack in the education sector. In 2023, Trustwave researchers monitored 352 ransomware claims against educational institutions.[8] While the specific tools used by attackers varied, each campaign followed the same steps, from gaining the initial foothold, to downloading tools and malware into the system, expanding into larger segments of the system, and exfiltrating data.

Phishing stood out in the Trustwave study as the most commonly exploited method for gaining an initial foothold in an organization. Instead of attempting to exploit vulnerabilities in the software or systems on the network, it was easier for attackers to target staff, faculty, or others who have access to systems within the institution, including access to finance systems and databases, which would include PII on students. Phishing pretext in this case may include scenarios of fake university communications, enticing job or grant offers, that require the victim complete certain tasks or provide sensitive information.

Typically, the attacker is "phishing" for one of three objectives:

- Credential theft, achieved by tricking the user into entering their login information
- Malware insertion, which occurs when the user clicks on or downloads an attachment containing PowerShell scripts or JavaScript, or enables macros in a document
- Other actions, such as persuading the user to disclose confidential information or perform actions under the false belief that they are applying for a student job or engaging in a university-related process.

In the education sector, the Trustwave study found that the most common types of email attachments used for malware distribution are HTML files, executables, and PDFs. HTML attachments make up 82% of malicious email attachments. These attachments are primarily either a standalone HTML page where someone "logs in" and provides the attacker with credentials to enter the system, or feature redirects to a malicious site.

CASE STUDY

In a recent phishing scheme targeting universities, attackers sent emails disguised as "requests for quotations" from educational institutions. The emails featured the university's logo and spoofed the university's name in the "From" and "Subject" headers, as well as in the filenames of the attachments. The university's "annual budget" was attached for review; the attachments included malicious executables or archives containing malicious executables. The executables delivered through phishing campaigns included the notorious Lokibot Infostealer, Agent Tesla RAT, and Downloader Guloader.

8 2024 Education Threat Intelligence Briefing and Mitigation Strategies, Trustwave Threat Intelligence, February, 2024, https://www.trustwave.com/en-us/resources/library/documents/2024-education-threat-briefing-and-mitigation-strategies/

What Can Be Done

The most effective step an educational institution of any size or level can take to secure vital and sensitive data is to ensure that all individuals—whether students, teachers, researchers, or cafeteria workers—who access the system are equipped with the proper tools to protect their "window" into the system, ensuring that only they can access it.

After an exhaustive study of attacks and breaches across sectors, the 2024 Verizon DBIR[9] concluded with:

This is probably cliché at this point, but we're believers that the first line of defense for any organization isn't the castrametation [designing and laying out] of their systems but the education of their key staff, including end users. Fortunately, this isn't simply us standing on our "user-awareness" soapbox. We have both figures and hard numbers to help quantify our stance. The first lesson to learn is that phishing attacks happen fast. The median time to click on a malicious link after the email is opened is 21 seconds, and then it takes only another 28 seconds to enter the data. That leads to a frightening finding: The median time for users to fall for phishing emails is less than 60 seconds.

Some good news is that, as an industry, we seem to be getting better with regard to phishing test reporting. More than 20% of users identified and reported phishing per engagement, including 11% of the users who did click the email. This is another impressive improvement and one that we desperately need in order to catch up with the previous year's increases in phishing and pretexting.

9 "2024 Data Breach Investigations Report," Verizon Business, n.d., https://www.verizon.com/business/resources/reports/dbir/

KnowBe4's PPP: The education sector

Each year, KnowBe4 carries out initial phishing security tests within organizations that have not run any security awareness training from our platform. The tests are conducted without prior alerts, on individuals performing their routine work tasks without any specialized training. These tests result in a baseline "Phish Prone Percentage," or PPP, that shows the percentage of employees that are prone to clicking on a phishing link. This is further broken down and applied to specific industries and geographic regions.

Spanning all industries and organizational sizes, the 2024 KnowBe4 Phishing by Industry Benchmarking Report[10] found that in the education sector specifically, the baseline PPP for small organizations with 1-249 employees was 33.4%. In other words, roughly one out of three employees were likely to click on a phishing link. For institutions with 250-999 employees, it was slightly better, at 31.2%. For large educational institutions with more than 1,000 employees the baseline of employees likely to click on a phishing link was 31.7%.

After 90 days of an integrated approach of educational content along with simulated phishing tests, the picture changed, with PPPs for the education sector reduced to 19%, 19.4%, and 18% respectively.

After one year or more of sustained training and simulated phishing evaluations, the year-over-year findings reinforce the impact of a steady, well-developed security awareness training program. In education, the average PPP for small institutions with sustained training dropped dramatically, to 3.9%. For medium sized organizations the average PPP after one year had dropped from an initial 31.2% to just 5.2%, while large organizations now dropped from an initial 31.7% to just 4.9%.

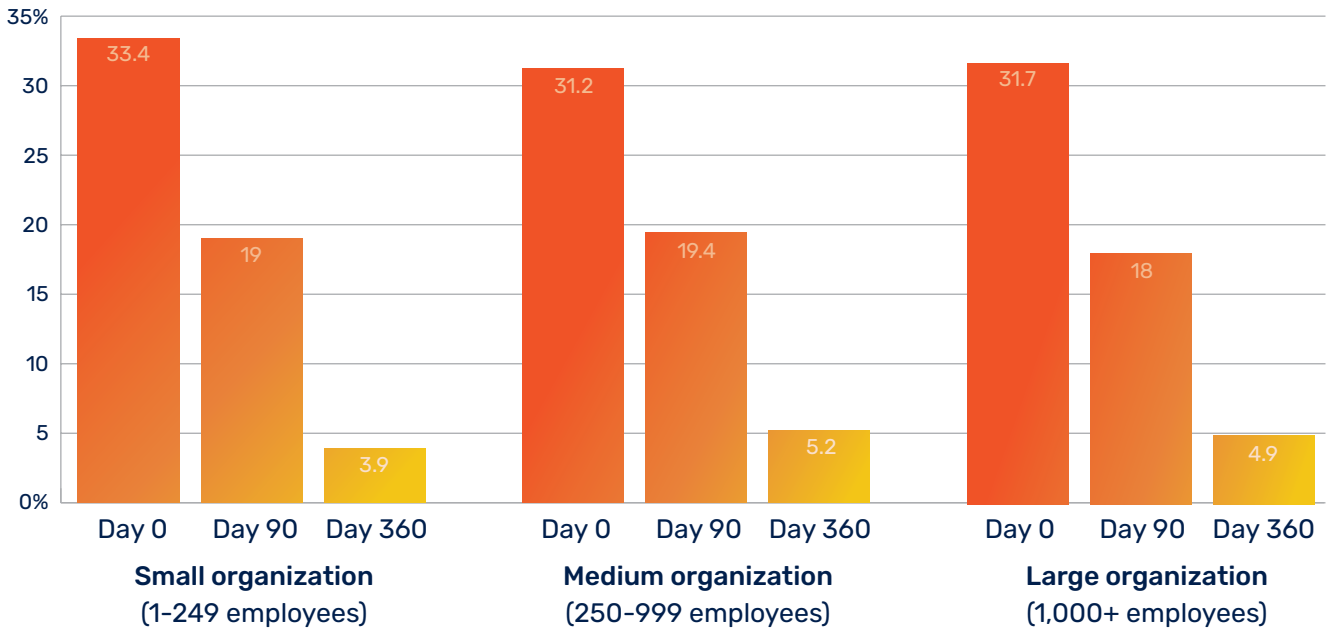


Fig.4 Effective training lowers phishing click rate in the eduction sector

Learn more about what KnowBe4 customers say

Customer Testamonials

10 "2024 Phishing By Industry Benchmarking Report," KnowBe4, https://www.knowbe4.com/resources/whitepaper/phishing-by-industry-benchmarking-report

About KnowBe4

As the provider of the world's largest security awareness training and simulated phishing platform, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud, and other social engineering tactics through a new-school approach developed by an internationally recognized cybersecurity specialist.

Join more than 70k international organizations in trusting the KnowBe4 platform to strengthen your security culture and reduce human risk.

For more information, please visit
www.KnowBe4.com

Additional resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com

0325US