CAMPUSGUARD®

CYBERSECURITY AWARENESS TOOLKIT

Inside the Cybersecurity Awareness Toolkit:

- Cybersecurity & Higher Ed Stats
- Cybersecurity Best Practices Checklist
- Cyberattack Methods
- Phishing: How to Prevent Your Employees from Taking the Bait
- Cybersecurity Bingo

CYBERSECURITY & HIGHER ED STATS

$447K

The average cost of a ransomware attack in higher education in 2020

$1.42M

The remediation cost following an attack in the education sector

95%

Of cybersecurity breaches are caused by human error

WHY IS HIGHER ED TARGETED?

Personal Data: Higher education institutions manage large amounts of sensitive personal data for students such as Social Security numbers, financial information, and medical records.

Slow Recovery Times: According to a report by Sophos, higher education had the slowest recovery times following an attack among all sectors in 2021. Forty percent took more than a month to recover.

Outdated Systems: Many higher education institutions rely on legacy technology and systems that can leave them vulnerable to cyber attacks.

Untrained Users: Oftentimes, higher education does not have a formal process to regularly train their users in security awareness. As a result, many users unknowingly download malware on their personal devices or applications through phishing attacks.

Remote Usage: Staff and students may be connecting to campus through unsecure wireless networks with their laptops or mobile devices. This can enable attackers to gain access to their devices, network, and data to launch a malware attack on their device.

CAMPUSGUARD®

CYBERSECURITY BEST PRACTICES CHECKLIST

Adhering to the following best practices can significantly reduce the risk of you becoming a victim of a security breach.

Update Operating Systems and Anti-Virus Software

Ensure your operating system is set for automatic updates, and reboot your system regularly. Anti-virus and anti-malware programs should automatically check for updates and scan your devices.

Use Strong Passwords

Use complex passwords or passphrases, at least 8 characters with a combination of upper and lower case letters, numbers, and special characters. Change your password at least every 90 days and don’t reuse passwords across multiple systems. Do not share your password with others.

Least Privilege Access

Only those individuals with a specific need to know should be authorized to access sensitive information. Use the principle of least privilege which limits users' access rights to only what are strictly required to do their jobs.

Maintain an Accurate Inventory

Know where sensitive information resides and keep track of servers, workstations, mobile devices, back-up systems, etc.

Secure Devices

Any device that holds sensitive information should be locked when not in use and encrypted. Don’t misplace devices or leave them vulnerable to theft.

CAMPUSGUARD®

CYBERSECURITY BEST PRACTICES CHECKLIST (CONTINUED)

Secure Information Disposal

All paper documents containing sensitive information should be shredded. Electronic media must be thoroughly reformatted or physically destroyed.

Back Up Data

Can you retrieve back up files of data or copies of critical information? Ensure you have an approved system in place to store and secure your valuable data files.

Secure Transmission

Do not send sensitive information via unencrypted email or other unsecured messaging methods.

Email Awareness

Be skeptical of emails and do not click on or open suspicious attachments or links. Only open emails from a trusted source.

Connect Securely

Only connect to trusted, private networks. Do not connect to public Wi-Fi networks.

CAMPUSGUARD®

CYBERATTACK METHODS

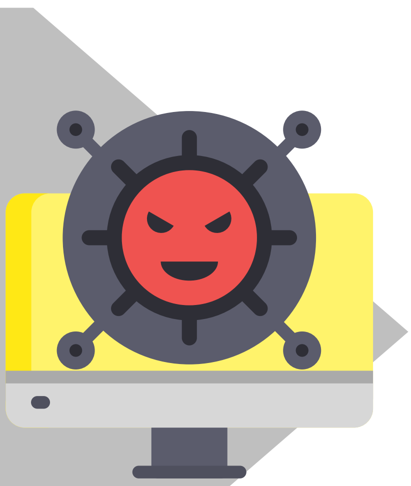
Many companies lack strong cybersecurity practices in place, making them vulnerable to data breaches

To combat cyberattacks, organizations need to include cybersecurity awareness, prevention, and data security best practices as part of their culture.

Here are some common methods that hackers gain access to your organization's networks.

Malware

Malware is malicious code or software inserted into a system that compromises the availability, integrity, and confidentiality of data. It can cause widespread damage and disruption to your organization.

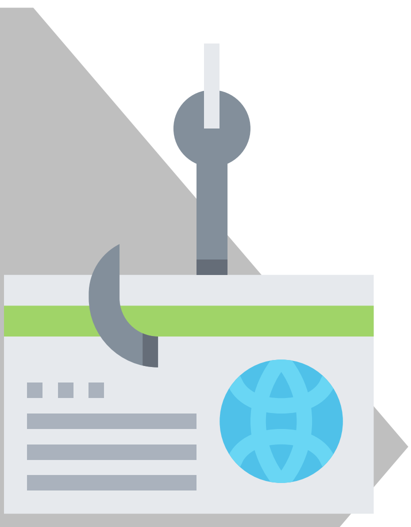


Ransomware

One of the most widely-used methods of attack, ransomware infiltrates computer networks and encrypts files using public-key encryption. It prevents or severely limits users from accessing their system by malware. To regain access to your data or system, ransomware will ask you to pay a ransom using an online payment method.

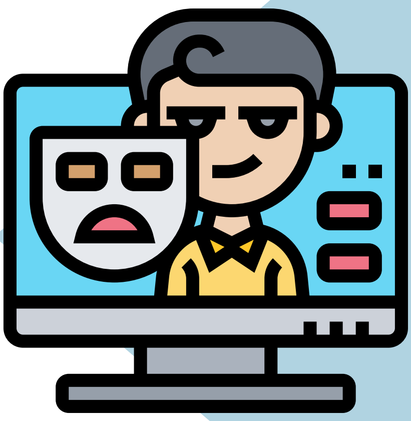
Phishing

Phishing, a form of social engineering, occurs when someone attempts to access sensitive information. Phishing emails usually come from someone posing as a trustworthy person or company you do business with. The email often requests a response, sometimes urgently, by following a link to a fake website or email address where you will provide confidential information.



CAMPUSGUARD®

CYBERATTACK METHODS (CONTINUED)

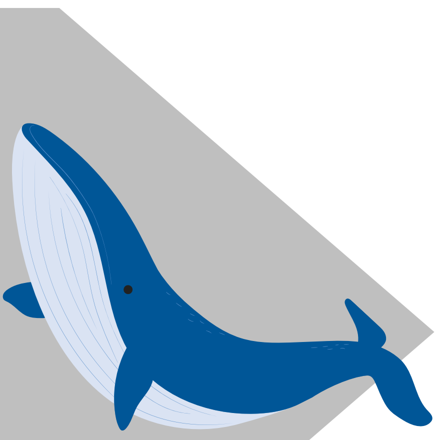


Spear Phishing

Spear phishing is a more targeted attack directly toward an individual or smaller group to gain access to confidential information. The attacker gains access to an individual's email account and sends an email to other individuals, posing as a trusted source.

Whale Phishing

Whale phishing targets high-profile employees, such as the CEO or CFO of an organization. Oftentimes, the attacker will impersonate the CEO to solicit personal or corporate information, or carry out financial transfers.



DDoS Attack

A "Distributed Denial-of-Service" (DDoS) attack occurs when an attacker floods a server with internet traffic to prevent users from accessing connected online services and sites. In some cases, perpetrators install ransomware on their servers and demand a large sum of money before reversing the damage caused.

Password Exploitation

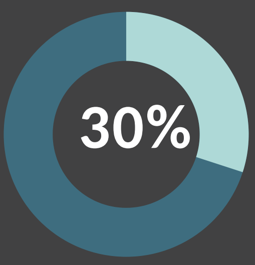
Passwords that are weak, easily guessable, or used in credentials across other sites can enable intruders from entering your organization's environment. Many organizations fail to notice the misuse of compromised accounts, putting its network at serious risk. Whenever possible, use a password vault or manager to ensure that your passwords are stored securely.

CAMPUSGUARD®

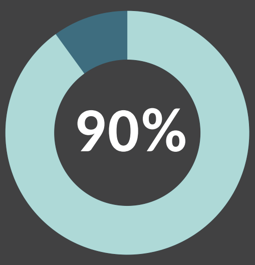
Gone Phishing

How to Prevent Your Employees from Taking the Bait

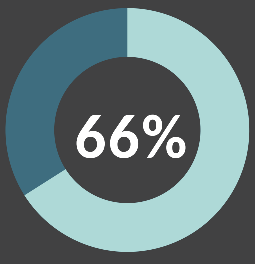
Specially crafted, seemingly legitimate-looking emails used to trick employees into providing confidential data (usernames, passwords, payment card details)



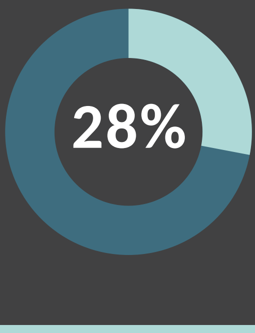
Phishing emails that are opened



Security incidents involving phishing



Malware installed via email attachments



Phishing intended to steal financial data

Consequences of Phishing

- Malware infections
- Compromised accounts
- Loss of data/money
- Loss of productivity
- Employee disruption

23.7 days

Average time to resolve a cyber attack caused by phishing

$4.65 million

Annual cost of phishing for average organization

Easy Targets

Employees are:

- Distracted
- Multi-tasking
- In a rush
- Eager to please

Questions employees should be asking:

Why have I received this email?
Does the link go to the correct location?
Is it from someone I know?
Was I expecting it?

Only 1 in 5 employees report phishing emails.

Fun fact: Employees are more likely to report phishing in the morning and in the middle of the week. "It's Friday...not my problem!"

Awareness Works

Preparing users and getting them to think before they click will lower the response rate.

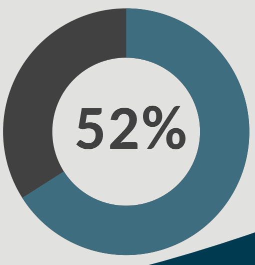
- 15% of users who fell victim once, took the bait a second time.
- Only 3% clicked more than twice.

Phishing Simulations

- Securely test your users
- Identify recipients who click or open
- Provide education
- Reward those that report e-mail to IT

Organizations quantifying a reduction in phishing susceptibility after:

- Phishing simulations
- Awareness training
- Ongoing awareness



CAMPUSGUARD®

To learn more about CampusGuard's phishing simulation testing, contact crm@campusguard.com.

CYBERSECURITY BINGO

How many of the following words do you know?

Score 1 point for each definition you know. Add up your correct answers, and check your score below.

PHISHING e-mails that appear to originate from a trusted source	**BRUTE FORCE** attack method involving an exhaustive procedure that	**ENCRYPTION** encoding a message or information in such a way that	**BIOMETRICS** use of physical characteristics of users to determine	**CRIMEWARE** malware used by cyber criminals to infect systems for financial gain
IDS (INTRUSION DETECTION SYSTEM) gathers and analyzes information to identify possible security breaches	**BOTNET** a large number of compromised computers that are used to create and send spam or viruses	**PATCH** update released by a software vendor to fix bugs in existing programs	**MALWARE** software that appears to be usefull, but actually gains unauthorized access to system resources	**SEPARATION** OF DUTIES splitting privileges among multiple individuals or systems
VIRUS hidden, self-replicating malicious software that infects other programs	**AUTHORIZATION** the approval, permission, or empowerment for someone or something to do	CAMPUSGUARD®	**DICTIONARY** ATTACK attack that tries all of the phrases or words in a dictionary, trying to crack a password or key	**RANSOMWARE** forcing a victim to pay a ransom to decrypt compromised files and regain access
DUMPSTER DIVING searching through discarded media for sensitive information	**MASQUERADE** ATTACK attack in which one system entity illegitimately poses as another	**SNIFFER** a tool that monitors network traffic as it is received in a network interface	**WAR DRIVING** process of traveling around looking for wireless access point signals that can be used to gain network access	**KEY LOGGER** Software or hardware that tracks keystrokes and keyboard inputs
WORM computer program that can run independently and propagate itself onto other hosts on a network	**SQL INJECTION** SQL code is inserted into application queries to manipulate a database	**PASSWORD** passcode used to confirm the identity of a user	**ZERO DAY** the day a new vulnerability is made known, no patch is available yet	**IDENTITY THEFT** deliberate use of someone else's identity, often for financial advantage

How did you do?

Scores:

CyberSadness
1-10: You have heard of cybersecurity, right? You could definitely brush up your skills a bit. We know you can do it!

CyberCharmer
11-20: You speak fluent cybersecurity, but have room to learn more. We're definitely impressed, though!

CyberNinja
21-25: You have an impressive portfolio of cybersecurity knowledge. You may be the nerd of your friend group, but you're the least likely to get hacked. Congratulations!

CAMPUSGUARD®

CYBER THREATS ARE EVERYWHERE. WE CAN HELP.

We have the security and compliance solutions you need to safeguard your institution from a potential cyber attack.

- Annual Support Agreement
- Compliance Support
- Customer Compliance Portal
- Incident Response Plan
- IT Security Assessments
- Online/In-person Training
- Penetration Testing
- Vulnerability Scanning

Visit CampusGuard online

Contact our Sales team

CAMPUSGUARD®