EXPEDE
CONSULTING

2022

THE BENEFITS OF CYBER SECURITY AWARENESS TRAINING WITHIN UNIVERSITIES

CYBERSECURITY IN 2022

Cybersecurity has never been more important. Over recent years, cybercrime, accelerated by the covid crisis, has reportedly increased by over 600%. Almost half of businesses (46%) and a quarter of charities/organisations (26%) report having cyber security breaches in the past 12 months alone. The numbers will be even higher as many crimes go undetected. The cost to businesses is huge: Ransomware attacks cost UK businesses £71 million in downtime alone, and a phishing attack to a mid-sized organisation costs £1.3 million on average. Cybercrime is arguably the world's biggest criminal growth industry, with an expected toll of over £5 trillion globally.

95% OF CYBERSECURITY ISSUES CAN BE TRACED TO HUMAN ERROR

World Economic Forum Global Risk Report 2022

HIGHER EDUCATION ATTACKS

In 2020/21, as universities moved online in the light of the pandemic, a huge number of new risks arose. Universities have always been at high risk of cybercrime, with student data, personal information, and extremely valuable research making institutions prime targets for cyber criminals.

This is why 75% of data breaches in the education sector happen at universities alone. Ever since the infamous security attack of 2018, where Iranian hackers targeted over 300 institutions, attacks on universities have continued to rise. During the pandemic, it seemed almost every week a new attack had occurred, with some UK institutions having to shut down their services for 2 weeks or more following an attack.

Now, over 25% of universities have admitted to having highly confidential data stolen, including national defence and medical research, and 87% have experienced at least one successful cyber-attack. Phishing attacks on students have also continued to increase, and it is no surprise universities now rank cybercrime as the most crucial risk they face.

THE MAJOR PROBLEM IN HIGHER EDUCATION

The major problem is not always due to lacklustre cybersecurity systems or defences. In fact, **over 90% of cybercrime incidents are now caused by criminals targeting staff (or students)**. This is often through phishing attacks, where individuals are targeted with fraudulent communication that tricks them into clicking bad links, handing over sensitive information, or installing malware. Phishing is often done through email, and new data suggests over half of internet users receive a phishing email every single day.

These attacks are easily preventable. 97% of people around the globe cannot identify a phishing email, and 74% would download a potentially malicious file because they lack the cyber awareness to spot and prevent it. At universities, **if students and staff were given appropriate training, it would rapidly cut down the number of data breaches and successful phishing attacks**.

On average, 30% of users within higher education have fallen for phishing emails, which makes it no surprise that the sector often ranks last out of all industries in terms of cyber security preparedness.

THE SOLUTION

Human error is by far the biggest cause of security incidents and tackling this is key to reducing attacks within the sector. Security Awareness Training is by far the best place to start. Training staff and students with the information required to recognise (and react to) cyber threats, will cut the problem off right at the source, and immediately prevent cyber-attacks from developing in the first place.

TYPES OF ATTACK

Universities, much like any other business, are at constant risk of cybercrime.

However, unlike other businesses, universities have a far more complex ecosystem, including different agents (students, staff, third parties), different spaces (virtual learning environments, Zoom or Teams calls, university-specific emails, physical Wi-Fi hotspots, libraries/study areas), and of course extremely valuable data that needs to be protected. But what are the major types of cyber-attack universities face?

Phishing

Phishing is one of the most common forms of cyber-attack. Most university users have their own university email which is rarely sent anything other than work-related or other important documents. Phishing emails sent to these accounts can be extremely convincing. In the past few years, phishing attacks have increased by over 100%, with remote work and the requirement to constantly be clicking online lecture links or portals can make it easy to fall victim.

Data suggests 30% of students have fallen for phishing emails, but as with all these things, the likely number is much higher.

Phishing can take many forms, such as Business Email Compromise (BEC), where a specific person within an organisation is impersonated (including using a similar or compromised email), which makes it extremely difficult to tell the fake email apart. Emails can contain malware, can lead you to scam links, or can result in your passwords/data being stolen.

Other types of phishing, such as 'whale phishing attacks', target a specific member of an organisation. If someone with administration access at a university, or someone with access to the cloud and learning services, is successfully targeted, then the results can be far more devastating.

Overall, phishing relies on a lack of understanding.

Most people can’t identify a phishing email, which means they can easily fall victim to these scams. If students and staff members have the correct training to understand how to tell if an email is fake, including looking at link URL before clicking, examining the 'from' address to ensure it is genuine, and checking for obvious signs of foul play, then phishing attacks could be almost completely avoided.

Malware

Malware refers to any type of malicious software designed to harm or exploit a device or network. Malware attacks require a certain type of software to be installed onto a device, which usually means a user must click on a link. Without even realising it, the user can then be compromised, and their device is no longer safe.

There are several malware attacks, including MITM (man-in-the-middle), trojan horses, ransomware, spyware, and more. Ransomware attacks are some of the most costly, where systems are taken down by hackers and not returned until a ransom fee is paid. A number of universities across the US were taken offline in April 2022 due to a ransomware attack, and online exams were severely disrupted. Similar incidents happened in the UK during lockdown, costing up to £2 million for a single malware/ransomware attack.

From a student perspective, malware such as spyware and keyloggers can be used to steal passwords, emails, and other personal data. Again, simply clicking on the wrong link or visiting a compromised website is all it takes for code to be installed on a device, and from then on, a student can lose all their passwords and personal data.

Like phishing, malware is usually the result of human error.

The best way to prevent malware attacks is through education. If a student or staff member knows what to look out for, understands the precautions they should take, and can see potentially compromised links before clicking on them, then most malware attacks could be prevented. Of course, having the correct device security and protection is important, but without an understanding of malware in the first place, a student can never be completely safe from attack.

Password Security

Hackers don't just use spyware to steal your passwords and data, poor passwords can be hacked physically or with a program, without even needing malware on your computer. **Over 60% of people use the same password for multiple accounts**, meaning a hacked or leaked password could cause severe damage to the victim.

There are many ways to avoid this, including using different passwords for each account or using password generators to ensure they cannot easily be stolen. Multi-factor authentication (MFA) is another crucial way to protect an account. Even if a password is compromised, a hacker will not be able to access your account without having the security code texted to your phone. Fortunately, many universities have implemented MFA, particularly for their emails.

DDoS Attack

Although human error is involved in most cyber-attacks, this is not always the case. Sometimes a targeted attack can occur that is not so easily avoided. A distributed denial-of-service (DDoS) attack happens when systems and servers are overwhelmed by hackers to the point where they can simply no longer operate, resulting in entire networks, websites, or learning platforms being shut down.

Whilst these types of attacks are harder to avoid, there are still many things a university can do, such as having an appropriate firewall in place to detect requests to a site to make sure they are legitimate. This can help stop the attack in its tracks before it starts to happen.

Similarly, having an overarching cybersecurity strategy and plan will make sure that universities know exactly how to react to and recover from an attack, reducing its impact.

Again, however, many DDoS attacks occur through compromised devices within the network, meaning malware has probably been installed on them before the attack takes place. If students and staff were properly educated on the issues of phishing and malware, then their devices would not be infected, and the DDoS attack may never happen.

AWARENESS CAMPAIGNS & TRAINING

It is estimated that between 85-95% of all breaches are due to human error. Phishing, malware, and password security are key issues that could usually be easily avoided. Even DDoS attacks could mostly be avoided if internal devices were not so easily infected.

The easiest, fastest, and most affordable way for universities to combat cyber security issues is through awareness campaigns and cyber security awareness training – by improving the capabilities of the ‘human firewall’.

What are awareness campaigns?

Security awareness campaigns are efforts designed to improve cybersecurity knowledge amongst users within an organisation. It educates users about the cyber security landscape, helps raise awareness of threats, and teaches users how to avoid cyber-attacks as best as possible. The idea is to create a 'culture of security compliance' within an organisation, putting cybersecurity at the forefront of users’ minds when using a device or accessing their email.

The reason it is often referred to as a 'campaign', rather than simply 'training', is that cybersecurity campaigns go much further than an educational one-off. Campaigns should aim to put cybersecurity as a key part of the organisation, receive appropriate investment, have regular discussions/updates, and be tailored to each team member's role and security level.

At a university, staff and students should always be involved in the awareness campaign. From the initial consultation to regular training and testing to detailed case studies and test scenarios, a thorough campaign will cover every aspect of cybersecurity.

The end goal, of course, is to ensure students and staff will be able to recognise the dangers and respond appropriately when they are faced with them, in order to significantly reduce the chance of a cyberattack.

In the next section, we will discuss the crucial aspects that a successful awareness campaign should involve. However, here are some of the most common exercises that awareness campaigns across the world will use:

79% use computer-based awareness training.
68% use phishing simulation exercises.
46% use awareness campaigns (videos and posters)
45% use in-person security awareness training.
38% use monthly notifications or newsletters.

In reality, a well-designed programme should include all of these elements. Whilst it comes as no surprise that computer-based awareness training forms most training programmes, the fact that almost **1/3 of programmes fail to make use of phishing simulation exercises** is concerning.

Without seeing and practising in a more ‘real-world’ scenario, it will be difficult for students (or staff) to be able to put what they have learnt into practice.

What should an awareness campaign involve?

Awareness training should not simply provide materials to teach staff and students about cybersecurity, it needs to be far more detailed than that. When surveyed, only 37% of staff enjoyed their cybersecurity training. Whilst being enjoyable is not a key factor, making the training as interesting, comprehensive, and engaging as possible will help to hammer the key ideas home. As such, awareness campaigns should involve a wide variety of training techniques, topics, and tests to keep users on their toes.

Some of the key aspects of an awareness campaign that are required in order to ensure a comprehensive understanding of cybersecurity issues within a higher education organisation include:

The Training

The initial training should cover a wide range of topics. The very best campaigns will tailor each campaign to the correct individual. For university staff, an understanding of GDPR compliance would be crucial. Staff have access to personal student data, and ensuring this does not become public should be a key part of their training. For students, examining issues such as phishing attacks and avoiding malware will likely be more important.

Training must be targeted to the user, which is why the best training programmes offer a variety of options to suit each individual department/faculty. Whatever the case, training should take a mixed approach. Video content, written guides, posters, end-of-topic tests, games/scenarios, and constant feedback should all be part of the training, as this has been proven to be far more impactful that a single-media approach.

Simulated 'test' scenarios – the most important aspect of a campaign is testing users with simulated phishing emails and scams. Various studies (Tidwell, 2011) have shown that simulated scenarios, combined with awareness training, lead to better results than simply providing the initial training. Simulated scenarios involve a ‘fake’ phishing email, sent to users, in order to determine whether or not they will click the scam links. When sent out to users at random, this can be extremely effective in determining how much they have learnt from their initial training. It can also help identify the staff and students who still require more training, and cost-effectively target training at the individuals who need it the most.

The Cultural Shift

Awareness campaigns will not work unless everybody is on board. Often it is decision-makers who believe that IT security and awareness training is important (96% agree with this).

However, as you go further down within an organisation, the perceived importance diminished. In fact, **only 63% of other employees believe that cybersecurity issues are important**. At a university, it is likely that this number will be even lower, with many students not feeling concerned with the general cybersecurity issues a university may face. A cultural shift is absolutely necessary. Everyone must be involved with the training, and the leaders within an organisation must convey the importance of this training to everyone else.

Results

As with any aspect of an organisation, awareness campaigns must be results-driven. Goals must be set out, and targets hit, in order to prove the effectiveness of the programme. The very best awareness training will deliver regular updates on the progress of its users. Regular tests must be taken, and simulations must take place at various intervals, providing constant feedback to the university as to which students and staff members require further training.

Many training programmes offer certificates or other incentives to try and encourage participants to improve their knowledge, and this is certainly something universities should be looking into.

HOW CAN REGULAR AWARENESS CAMPAIGNS HELP UNIVERSITIES?

There are many examples of success stories from institutions that have successfully implemented awareness campaigns in their organisation.

A college in the US, for example, reported a significant reduction in malware and viruses, a 90% reduction in successful phishing attacks, significantly fewer support requests, an increase in the number of users reporting incidents and attacks, and a greater awareness of security issues, all after their awareness programme was introduced. When looking at specific results (Mimecast, 2021), you can see the difference:

General phishing emails – 600% increase in capability of detecting phishing after SAT
Business Email Compromise – 300% increase in capability of detecting compromise after SAT
Web or Social Scams – 250% increase in capability of detecting web scams after SAT

Regular awareness campaigns have been proven to dramatically improve cybersecurity awareness among individuals, reducing successful phishing attacks by between 80-90%, and resulting in far fewer financial and PR damages for universities.

At Expede, we work with several security awareness training partners that take different approaches - from supplying the platform and content for your teams to managing campaigns. at one end of the spectrum, to those that provide a fully managed service at the other.

Each partner offers cost-effective and results-driven training that covers all the crucial aspects of a successful programme, including mixed-media content, simulated test scenarios, and real-time results and feedback to identify problem areas.

Get in touch to find out how the team at Expede can help deliver the right cyber security awareness programme for you. Email your Virtual Chief Information Security Officer at

vciso@expede.consulting