THE ULTIMATE GUIDE TO PROTECTING AGAINST PHISHING ATTACKS

Cyber Risk Aware

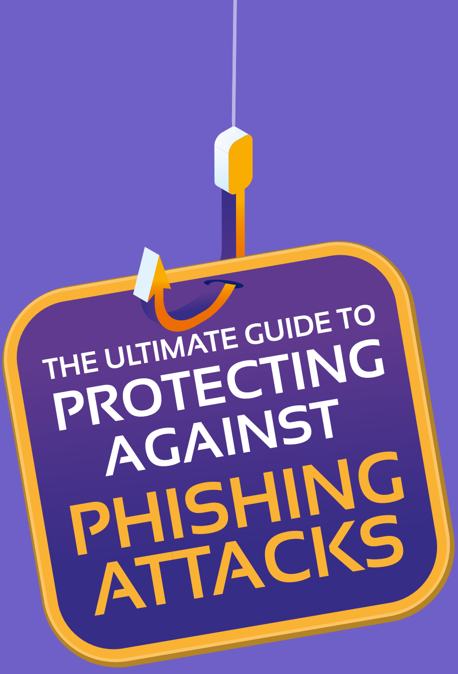
Creating your human firewall!

Cyber Risk Aware

Creating your human firewall!

Cyber Risk Aware

Creating your human firewall!



THE ULTIMATE GUIDE TO PROTECTING AGAINST PHISHING ATTACKS

Index

Cyber Risk Aware

Creating your human firewall!

Introduction

In the real world we have developed practices to keep ourselves, our families and businesses safe from criminals. We lock car doors, secure home front doors, and you probably wouldn't walk down a dark alley in a strange city late at night not knowing where it was leading to.

Unfortunately, we are still only developing those equivalent best practices in our digital lives; and many are still at a loss to understand what to do. Saving your passwords in your browser, for example, is like leaving the keys of your car on the front seat so that you can find them easily when you return; and feel like heading alone down a dark alley, clicking on an unsolicited email link will get you there.

Companies have tried to protect against criminals by implementing various security technologies like Anti-Virus and Firewalls etc. This is all necessary but not sufficient. You would not leave your keys outside your house and expect the police to be successful in protecting them from falling into the hands of an opportunistic criminal. Research has shown that Spam/Phishing filtering software only has a success rate of 93%. Given the sheer quantity of Phishing E-mails in circulation at present, this gap of 7% ensures that a significant amount of Phishing E-mails end up in the inbox along with legitimate e-mail - and this is where the danger lies
The News tells us that Cybercrime is growing at an alarming rate. The success rate is also growing because Cyber Criminals now know to target staff and humans because it has been proven time and time again that they are your weakest link. With your reputation on the line the other critical fact to know is that the vast majority of cyber security breaches start with a simple Phishing attack. At its most simple phishing is carried out by a criminal impersonating another company or another individual for the purposes of extracting information from you that they then can use to either access your systems or steal your data.

This has been taken to a whole new level with Business eMail Compromise also known as CEO fraud. This is where the illegal attacker impersonates the CEO, President, or other C-level executive within a company, using their presumed status to gain access to privileged information such as customer data or bank accounts. These attacks can cost a company tens or even hundreds of millions of dollars, virtually overnight, such as when Ubiquiti Networks lost nearly $47M.

So, if your company uses eMail and you are not proactively working with your staff to help them avoid these threats, then you are taking a significant risk with your information.In order to help people, understand and mitigate these risks we put this paper together based on our experience. To guide you through this minefield we look at the following topics

- **Eight Quickest ways to Spot a Phishing Attack**
- **Five Key Steps to stop Phishing Attacks**
- **Six Elements of an effective Phishing Awareness Training Program**
- **How to build and deliver an effective Phishing Awareness Campaign**

After reading it you should be aware of the types of threats that are out there and the steps that you need to take to protect yourself against them. The blunt reality is this - technical defences alone won't keep you safe and you need to be investing in helping you staff recognise these risks in order to mitigate them. It has been shown too many times already that if you are not training your staff and assessing the level of risk in your organisation you will almost certainly fall victim to one of these attacks. Prevention is always better than cure.

[1] https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html

The Eight Quickest Ways to spot a PHISHING ATTACK

> *“97% of people cannot identify a sophisticated phishing email”*

Inspired eLearning

It is human psychology that makes Phishing Attacks effective for criminals.

According to the 2018 Verizon Data Breach Report, 4% of people will click on every single email without discretion. Amusement and Entertainment also figured strongly within the study of why people click on links.

Attackers know that if they can also link these emotional manipulation elements within their attack, they have a greater chance of succeeding.

Here are the key indicators that an eMail or Link may be part of a phishing attack

1. The Message Contains a Mismatched URL

One of the most obvious signs of a phishing attack and a malicious piece of content is that the content doesn't match the URL. But because many people are becoming wise to this type of clue, attackers are now changing the URL to match their message. However, in some cases, users will find that if they mouse over the URL, the URL doesn't match the text link. This is a significant sign of a scam and should be reported.

2. The URL Doesn't Match the Domain

Another trick employed by cyber criminals is to use a URL that doesn't match the domain of their site. For example, they might use the name of a legitimate company such as Apple or Microsoft in order to get the user to click on the link and go to their malicious content. The name of the legitimate company will be the main domain, and then the fraudulent company will be a child domain within the link. In this example, a user might see something like **"www.apple.scamwebsite.com"**.

3. The Sender of the Communication Doesn't Appear Legitimate

In some cases, it's possible to determine whether the communication involves a phishing scam simply by looking at the sender of the information. While phishing attackers are becoming better at disguising their address, there are still small differences between legitimate communications and fraudulent communications in terms of the email address of the sender. For example, the common PayPal phishing scam involves senders using Gmail or Hotmail email addresses, and not an original PayPal address.

4. The Content Contains Poor Spelling and Grammar

While most people aren't perfect when it comes to spelling and grammar, the vast majority can spot misspelled words and poor English if they look closely at the content. But many still miss this vital clue in addressing phishing attempts. In a legitimate piece of content, the style, grammar, and spelling will be checked by the writer and probably several other people within the company. But those producing spam and conducting phishing attacks don't always have the finest grasp of the language. They will misspell words and their sentence structure might not make any sense. Make sure employees read all communications carefully and look out for errors.

5. The Content Requests Personal Information

In an initial email to a client, a company will rarely ask for personal information to be provided. They might ask that the recipient subscribe to their communications or that they call company directly, but a bank, for example, will never require a customer to complete information via an email within its first initial communication. This is a common sign that the attacker is simply looking to extract as much information as possible from the target in the shortest amount of time.

6. The Action Wasn't Initiated by the Recipient

In cases where an email is received, and the initial contact was unsolicited, the communication is likely to be some form of spam. Legitimate companies will rarely send out first emails directly unless the recipient has signed up to a newsletter list or has agreed in some other way to the communication. For employees that receive emails seemingly out of the blue, it's important to look closely for signs of a potential phishing scam.

7. The Offer is Too Good to be True

We've all heard of the Nigerian Prince scam in which the recipient receives a letter from a member of the Nigerian royal family asking for a small loan, with the incentive of a large reward once the loan is paid. This is a clear example of a case in which the offer is too good to be true. A national lottery will not announce its winners via email. A long-lost uncle will not suddenly appear via email ready to give away their millions of pounds. If the offer is unbelievable, it's best ignored completely.

8. The Message Contains Threats

One of the most common phishing scams involves a message purporting to be from a government agency detailing a very specific threat against you or a member of your family. The communication might involve the recipient owing money to the government. Or it might detail other illegal activity that the recipient is said to be involved in. Inevitably, the sender will ask for money to resolve the legal issue. It's important to note that government agencies rarely send out email as their first form of communication and that threatening emails impersonating a government representative are an exceptionally serious crime in the UK.

Giving employees this knowledge can help to prevent organisations facing millions of pounds in losses over the coming years. The goal is to educate the individual and inspire them to notice the small details that could prevent a phishing attack from taking place. This commitment to education begins with the CEO and includes every member of staff within the company, each of whom has access to a computer on the company's network, and each of whom shares the equal responsibility for preventing phishing attacks. It's never too early to begin the education process and safeguarding the company against the most common phishing threats.

The Five Key Steps for Organisations TO STOP PHISHING ATTACKS

If you can't stop Phishing attacks on your company or employee's happening what can you do? The Research shows that training staff is the key difference in reducing your risk by up to 80%. Without that your technical defences will not be successful.

So, what are the things that the proactive business leader needs to do to help ensure that these attacks are not successful, they include;

1. Implement a Phishing Awareness Training Programme

No amount of technical defences will keep you secure, so have to focus on the source of the vast majority of successful attacks: individual error. Every individual requires information and education to help them detect threats, report them and ensure that future threats are prevented.

Implementing an effective training programme requires expertise and experience. In too many companies it is a tick in the box exercise. If you are using old content delivered in a traditional classroom environment you are probably wasting employee's time and your money. This is too important an area not to invest in the latest delivery of up to date content at the right time to your employee's

Working with an outside partner in this area has significant benefits, as they can help review your policies and results and provide as sense of how exposed you are versus other companies in your industry.

2. Run Simulated Phishing Campaigns

There is an old adage that what you don't measure you are not managing. Running effective simulations to test how Phish prone your staff are is key to understanding what needs to be done. Different industries are the focus of different groups and different threats. The ability to see if your training is reducing the propensity of your staff to click on phishing eMails helps to demonstrate that you are meeting your compliance obligations as well as giving you the peace of mind that what you are doing is having an impact. It also allows you to target users with additional help and training as needed making your overall efforts much more effective.

3. Make Sure All Systems Are Up-to-date

One of the most common reasons a phishing attack is able to take place across an entire network is that the company has failed to patch some of the flaws within their current system. To limit the damage caused by a phishing attack, make sure that all software is up-to-date and that the IT team has had a chance to review the structure regularly for potential issues.

4. Implement Comprehensive Spam Filters

While the latest commercial spam filters still won't catch 100% of the spam emails entering the company's email accounts, they will prevent the vast majority. It's important to note that the standard filters employed within Outlook and Gmail will not offer the requisite level of protection. They're simply designed to catch common spam messages, and not the newest and latest threats from phishing scams.

5. Harness Monitoring Software

Monitoring software should be used to highlight the potential for a phishing threat. The latest software is now designed to alert IT teams when a user clicks on a suspicious link or traffic levels differ significantly over a short period time. Software can also point to specific flaws within the company, helping teams to identify areas of concern and ensure that any common problems are resolved.

The Six Elements of an EFFECTIVE PHISHING AWARENESS TRAINING PROGRAM

Effective Phishing Awareness programmes have proven to reduce risk by up to 80% within six months, emphasising the point that you cannot depend on technical defences alone. Successful ones don't happen by accident, here is what they need to include;

1. Deliver the Right Content in the Right Way to the Right Users

Long classroom sessions where users are not engaged will not get the job done. Content needs to be delivered in digestible chunks preferably to the desk so that the User can absorb it. It needs to be constantly updated and kept fresh. If an element of gamification can be introduced even better. User attention spans are getting shorter all the time as the pressure of work and deadlines increases so content that is delivered in modules of less than 8 to 10 minutes has been shown to be much more effective. That does mean you need help scheduling and delivering that.

2. Simulation Phishing Campaigns

Gaining insight on the potential actions of employees is imperative for companies looking to implement a security training program. How will employees act and what will the impact be on the company due to these actions? Simulation phishing campaigns are ideal in this regard as they allow for a company's communication style to be mirrored and for phishing templates to be created. The resulting communication is then sent to employees at random, and their response is noted for risk assessment.

3. Corrective Training

As part of the testing phase, corrective training can be implemented to prevent the employee from making the same mistakes as they did in the test. During the corrective training, the experts will guide the employee on the mistakes they made and the potential impact their mistake could have on their company. The data shows this level of corrective training can help organisations build security-focused teams who are committed to eliminating phishing attacks.

4. Reporting and Tracking

Training teams can also offer reporting and tracking tools that identify weaknesses within the company infrastructure over the long-term. They can track stats such as the clicks on unsafe links and the number of viruses found on local computers. They can then use this data to highlight the changes being made within the company as a result of their training work. The reporting modules offered by the top training teams are also vital in guiding team leaders on training value.

Reports can be compiled into easy-to-digest data points that show the company's current security position and the progress made over previous months. This then helps makes the case for further security investment and gives decision-makers actionable data on their employees and their commitment to the training process.

5. Real-Time Threat Analysis

At the outset of the phishing awareness training program, it's important that the company has the tools to immediately identify threats to their system. At this stage, team members don't have a full handle on potential phishing communications and will need training and further guidance to protect the company. It's the time in training at which real-time threat analysis is essential. The real-time analysis can be used to monitor communications taking place on the network and alert IT teams when a potential threat arises. Once further training has been provided, there will be a reduced need for threat analysis in real-time.

6. Choose the Right Partner

In choosing a phishing training partner it goes without saying they need to be able to deliver previously highlighted elements. Increasingly you cannot do this in the traditional manner and you need a partner that can deliver an Awareness Training platform that makes delivery, scheduling, testing and reporting easy to deliver. Staff are under increasingly time and work pressures in today's competitive environments so this has to be frequent enough to be effective but without impacting unduly on productivity.

How to Build and Deliver an Effective Phishing Awareness Campaign

Based on the results of 1000's of simulated phishing campaigns here are the top 5 most effective practices you can implement to reduce your risk today.

Following these best practices can help you ensure your testing is effective and can maximise your return on investment in the long-term. While the phishing platform itself can provide a measured benefit of experience and expertise, and its latest features and tools, it is up to those within the company to hone each template and campaign to the needs of their organisation.

The best practices for a phishing awareness campaign include:

Understand the threat

The threat of phishing may be universal, but each industry will have a varied proportion of risk from a diverse selection of threat actors. Their motivations, intent, and even their applied methods and trends can be distinct, and therefore it is important to fully understand the who, the what, and the why before laying down your testing strategy. Select templates and techniques based on these threats, and your own experience of past phishing incidents.

Create a baseline

Metrics tracking is important to understanding your progress; after all it is by converting theory to practice and ultimately habit, that security consciousness is achievable. Know where you are beginning so that you can understand your current risk and thereby correctly strategize where you need to get to.

Typically, phishing testing begins with a simple (low sophistication) template and is advanced only when results show that mastery of a level has been achieved.
By beginning with a simple lure you can lay down a foundation of understanding at each level. Once a low sophistication template from one of the email topic areas (e.g. home/personal, business, or attachments) has been selected, it can be edited and customized to your particular needs.

Alternatively, some organizations like to launch their first campaign with a complex (high sophistication) email lure, and then use the high susceptibility results as validation for continued testing. There is nothing wrong in this approach, as long as subsequent tests go back to a lower sophistication lure so that learning can progress naturally.

Customise Your Feedback

Beyond the selection of an email lure template, the user feedback message is one of the most important pieces of a phishing testing plan. This “landing” page, which is either redirected to from an email lure template, or has been added as an attachment to said template, should at once communicate the error that was committed and simultaneously assure the recipient that the receipt was part of a secure test.

It is advisable to customize the user feedback message to include your corporate logo, and relevant corporate terminology. It is also best practice to share direct learnings based on the respective template. For example, call out the tell-tale signs of phishing that the email recipient should have identified: e.g. an inconsistent domain, a call to urgency, a promise too good to be true, or a threat too unrealistic. Offer as well relevant suggestions and tips: e.g. hover over hyperlinks to review a URL prior to clicking, or be sure of the legitimacy of an attachment prior to downloading and opening it.

The User Feedback Message is an opportunity to provide direct phishing avoidance training material to those identified as most susceptible. This opportunity can be extended with more formal training options like automatically enrolling susceptible individuals in required training, whether videos or computer based training options.

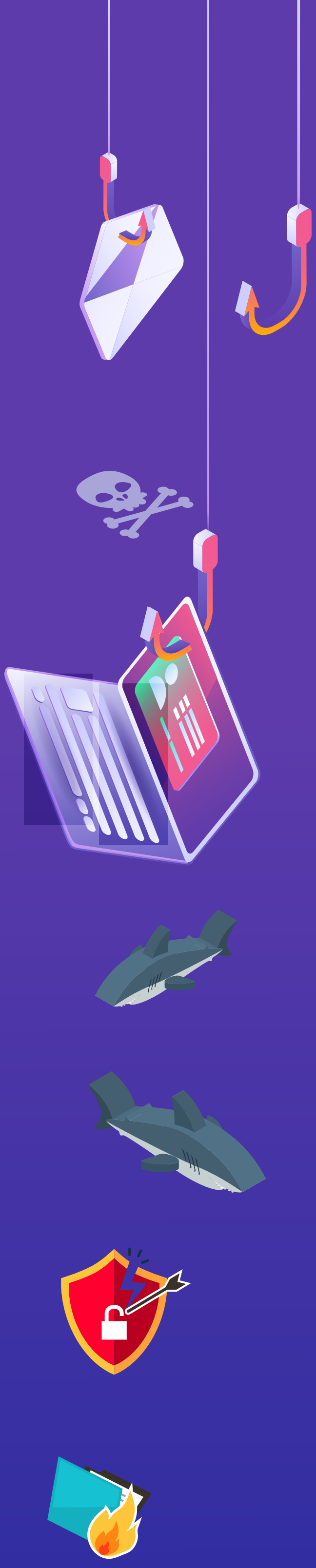
Track and Communicate

Phishing testing is not an exercise in instilling fear, and it should never be used as a means to ostracize or embarrass individuals. However, in order to understand the progress of security maturation, it is relevant to track, analyze, and communicate phishing testing results.

Firstly, determine what is relevant for you to track. Which variables will add to your understanding of corporate security and susceptibility? Information such as department, location, preferred languages, or even corporate rank may be especially relevant depending on the campaign.

Once data is gathered, it can be compared and tracked against industry benchmarks. Use available reports to gather additional data points, like operating system and browser version. Analyze your results from different angles and vantage points, then share your data summary with leadership and provide key learnings to the corporate body.

Some basic statistics that should be monitored include: overall susceptibility and the prevalence of repeat offenders. The phishing testing program could also be incentivized to offer rewards to those individuals who show themselves to be exceptionally resistant to phishing. Friendly competition can also be initiated between locations, regions, or departments, allowing for recognition of the most improved and least susceptible groups.



Set a Goal - Close the Gap

Once you have established a baseline, and begin to track your phishing testing results against industry benchmarks, it is important to set an improvement goal.

Working toward that goal will require practice, education, and awareness. Timely phishing testing provides the real-world simulation practice that will help email recipients hone their skills. It is important that testing occur steadily throughout the year, so that learnings aren't forgotten.

Additional training opportunities, to individuals through reactive campaigns, or more formal group training campaigns to identified deficient departments or locations, can provide the direct learning needed to curb susceptibility. If a plateau is reached further breakdown of data may be needed, to understand for example, if the device, way of working, or role may be playing a part in the increased risk.

If repeat offenders continue to click on multiple campaigns throughout a year, and initial training attempts have proven unsuccessful, it can then be appropriate to speak to the individual, their manager, and even Human Resources to create an individualized action plan. The follow-ups should be conducted in private so as not to shame the individual, and should be focused on improving understanding rather than punishing errors.

Increase Complexity

Once metrics show that employees are able to detect and react appropriately to their current phishing complexity level: including avoiding, deleting, and or reporting/ escalating phishing emails, it is appropriate to raise the level of phishing complexity.

Ensure a wide-ranging selection of phishing topics, types, and techniques as you increase the sophistication level. Routinely reassess the existing threat level and the propensity of risk associated with distinct threat actors, and hone your testing campaigns accordingly. Beyond the highest general sophistication level, it is relevant to employ techniques used in spear phishing, including incorporating corporate news and social media headlines.

The advantages of the Cyber Risk Aware Security Awareness Training Platform

Here at Cyber Risk Aware our comprehensive training platform has been used by Fortune 500 companies, FTSE 100 companies, and cyber insurance firms throughout the globe. Clients recognise the unique value the platform brings to their company and understand the threat of phishing is too significant to ignore. Our market-leading program includes:

Dynamic Simulations

Simulations should be designed to mimic in-house branding and communication styles so that even the most responsible employees can be tested. Our phishing simulations are considered the very highest quality.

C-Suite Attack solution

This is designed to tokenise the names of C-suite executives and then automatically populate phishing email templates. The simulations assess whether staff members will wire money or complete requested actions on behalf of the email sender, thereby highlighting their vulnerability to phishing techniques. Our Burst Mode enables a single phishing campaign to be crafted with multiple templates, which are then randomly delivered to staff. This helps drive the accuracy of the results from the training program.

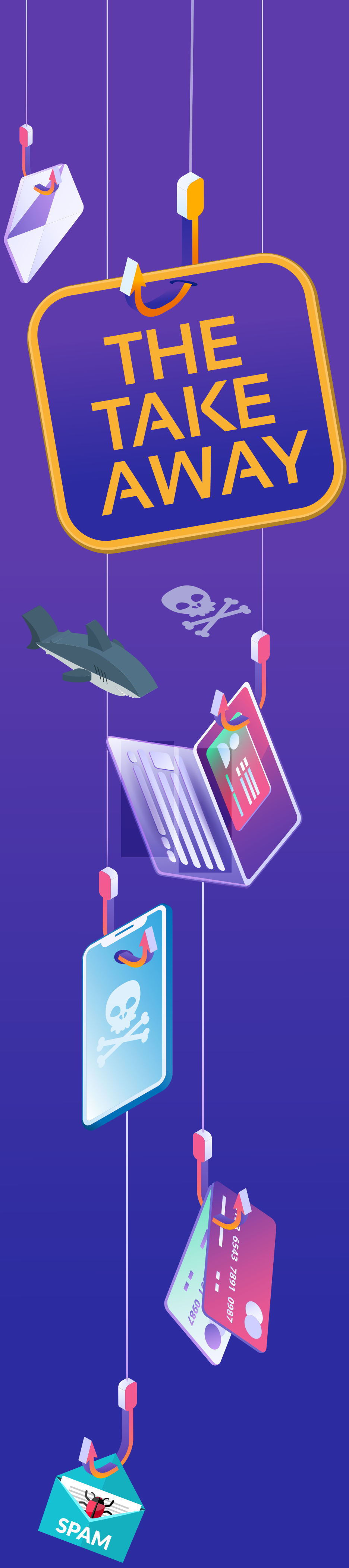
Alerts & Tracking

Our systems will alert management teams when a member of staff has clicked on a malicious link within an email or message. The alert will then allow management teams to take greater control over the training process, and ensure the user corrects their behaviour for the future. We also offer the finest tracking tools within the marketplace. Our tracking product identifies patterns of behaviour and helps determine the future role for training in the company.
Using our product, teams can track user response, identify areas for improvement across the company, and highlight the return on investment achieved during training.

Real-Time Alerts

Through effective monitoring of employee actions, our software includes real-time alerts that correspond with specific user behaviours. These alerts are designed to provide staff with content that details the danger in, for example, downloading a file from an unknown email sender. When the staff member receives the alert they're then given information on how to correct their behaviour. This process is completed confidentially to keep the member of staff in full control of their actions and to promote an autonomous approach to team security.

Cyber Risk Aware
Creating your human firewall!



The Take Away: You need to help your staff to secure your firm against Phishing

The research is clear: phishing is a growing problem and it's now costing UK companies millions of pounds a year. Those that don't prepare to face this threat will find their companies susceptible; and if they fall victim, they will experience a loss of public trust, a significant drop in productivity and, over time, a clear reduction of revenue.

The process of improving phishing security helps assure the survival of the company through the utilisation of industry-wide best practices.

Our team at Cyber Risk Aware has worked with hundreds of companies across the UK and the globe. We've worked with growing firms and multinational leaders of industry. And in each case, we've identified and then helped correct significant security flaws that could have caused long-term damage to their organisation and its customers. It's time for you to make a decision about your company and its market future. As we've shown, the threat of phishing has only grown stronger in recent years. Where once the threat came from a ragtag group of teens on a forum, now the threat is global and comes from professional crime syndicates with the dedication, tools and the knowledge to access vulnerable systems at will. What is your company doing to take a step towards full organisational protection?

We're here to guide you in this new and challenging security environment. Our training will focus on the individuals in your team and help each member make effective decisions for the betterment of the company and the security of your entire infrastructure.

CONTACT US

Cyber Risk Aware
Element 78,
George's Quay Plaza,
Dublin 2 Ireland

T: +353 1 9610016
E: info@cyberriskaware.com

Cyber Risk Aware

Creating your human firewall!

Cyber Risk Aware

Creating your human firewall!

CONTACT US

Cyber Risk Aware
Element 78, George's Quay Plaza, Dublin 2 Ireland

T: +353 1 9610016 E: info@cyberriskaware.com

cyberriskaware.com