PiSYS .net

A COMCEN COMPANY

Regular **cyber security training** gives your business the highest level of protection

We make IT easy

Two growing businesses were on very different paths: FitLife, an ambitious health and wellness startup, and NumberCrunch, a well-established accounting firm.

FitLife was thriving, full of energy and innovation. Their rapid expansion, however, came with a blind spot **– cyber security training.** The team was passionate and dedicated but had little awareness of how to protect the company's digital assets. Passwords were weak, emails were opened without scrutiny, and system updates were often neglected. Cyber security was not their priority.

On the other hand, NumberCrunch had a different approach. Though they were not a tech-driven company, they understood the importance of protecting their clients' sensitive financial data. With the guidance of their managed service provider, they invested in comprehensive cyber security training. Their training was hands-on, practical and tailored to real-world threats. Each employee learned to identify potential risks and respond quickly to protect the business.

One day, FitLife received an urgent email, supposedly from a trusted partner requesting sensitive information. Without hesitation, an employee responded, unwittingly granting cyber-criminals access to the company's systems. This phishing attack brought devastating consequences. Client data was compromised, business operations were disrupted and their reputation was severely damaged. The recovery process was long, costly and exhausting.

At the same time, NumberCrunch encountered a similar phishing email. However, their story unfolded differently. Thanks to their ongoing cyber security training, the team immediately recognised the signs of a scam. They reported the email to their IT team, who swiftly neutralised the threat before it caused any harm. NumberCrunch continued operating smoothly, their reputation intact, and their clients' data secure.

The journeys of FitLife and NumberCrunch highlight a key business lesson: **cyber security training is essential for every organisation**, not just the IT team. Even the most advanced software and security systems can only do so much. The true line of defence is a workforce trained to recognise and respond to threats.

PiSYS eCampus
A COMCEN COMPANY

At Pisys, we specialise in helping businesses protect their data by empowering employees with the knowledge they need. Our Pisys eCampus offers engaging, free cyber security training designed to keep your staff vigilant and your business secure. Contact Pisys on 01792 464748 or email hello@pisys.net to learn how we can strengthen your defences and safeguard your business.

The importance of cyber security awareness training

In today's digital landscape, businesses of all sizes face an increasing number of cyber threats. Gone are the days when only large corporations were targeted. Cybercriminals now recognise that small and medium-sized businesses can be easier targets, often due to limited resources and weaker security protocols. This makes cyber security training critical for every business, no matter the size.

Understanding the risks: Imagine arriving at your office to find all your computers locked with a ransom note demanding payment for access. This scenario, known as ransomware, is becoming all too common. The financial and reputational damage can be catastrophic, potentially leading to operational downtime, data loss and even legal consequences.

For some companies, the impact of a cyber-attack can be fatal. Take FitLife as an example. Their lack of cyber security training resulted in a serious data breach. Beyond the immediate financial loss, their reputation suffered long-term damage, impacting client trust and business relationships. It's clear that cyber security is not just a technical issue but a business-critical one.

The Human Element in Cyber Security: While technology can provide strong defences, it's often human error that creates vulnerabilities. Many cyber-attacks, including phishing, rely on exploiting human behaviour. Phishing attacks involve sending deceptive emails that trick employees into sharing sensitive information or downloading malware (malicious software).

Proper cyber security training can significantly reduce the chances of these attacks being successful. Employees trained to recognise suspicious emails, attachments and requests become your first line of defence. For instance, when NumberCrunch faced a phishing attempt, their well-trained staff immediately spotted the scam and avoided the chaos that FitLife experienced.

Cyber security is not just the responsibility of the IT department. From the CEO to the newest recruit, everyone in the organisation plays a role in safeguarding the company. Threats can target any department. An HR employee might receive a fake CV containing malware. The finance team could be tricked into paying a fraudulent invoice. Even the marketing department could be targeted through compromised social media accounts. Without cyber security training, any one of these scenarios could result in a serious breach.

The Need for Regular Training: Cyber threats are continually evolving and the tactics used are becoming more sophisticated. Training conducted a year ago may not cover the latest phishing schemes or ransomware variants. That's why ongoing cyber security training is essential to ensure employees stay informed about new threats and best practices.

NumberCrunch didn't just stop after their initial training. They invested in regular sessions to keep their staff aware of emerging risks. This proactive approach ensured their team stayed vigilant and prepared for new challenges.

At Pisys, we understand that an educated team is a secure team. Our eCampus provides comprehensive cyber security training that keeps your staff up to date with the latest threats. We offer free, short and effective training modules to help protect your business.

Implementing a Cyber Security Training Programme

Implementing an effective cyber security training programme for your business requires careful planning, execution and continuous improvement. By taking a structured approach, you can ensure your employees are well-equipped to recognise and respond to threats. Here's a three-step guide to help you get started.

Step 1: Planning Your Cyber Security Training Programme

Start by assessing your current cyber security risks. Identify your business's vulnerabilities by reviewing past security incidents and conducting a thorough risk assessment. Ask yourself key questions, such as:

- What are the most common cyber threats in our industry?
- Where are our security gaps?
- How aware are our employees of basic cyber security practices?

Next, set clear and measurable objectives. Do you want to reduce phishing email click rates? Improve password management? Ensure compliance with industry regulations like Cyber Essentials? Defining specific goals will help you structure your training for maximum impact. Once you've identified your goals, choose the right training methods. A mix of traditional and interactive approaches can cater to different learning styles. For example, online courses provide foundational knowledge, while phishing simulations offer practical, hands-on learning.

Finally, create a training schedule. Regular and ongoing training is crucial, as cyber security threats constantly evolve. Consider a programme that includes monthly online modules, quarterly workshops, and bi-annual phishing simulations. This combination keeps employees up to date and vigilant about the latest threats.

Step 2: Executing Your Cyber Security Training Programme

Begin by clearly communicating the importance of cyber security training to your team. Employees need to understand how their actions contribute to protecting the business. Gaining leadership support is critical, as management buy-in ensures the message is taken seriously throughout the organisation.

Next, ensure the training content is engaging and relevant. Use real-world examples and case studies to make the material relatable. Simplify complex topics and avoid unnecessary jargon. The goal is to make the training accessible to everyone, from the most tech-savvy employee to the least.

Hands-on activities are essential for effective learning. Incorporate phishing simulations and interactive exercises to give employees practical experience. This not only reinforces their knowledge but also builds their confidence in handling potential cyber threats.

Lastly, provide ongoing support and resources. Ensure employees have access to a knowledge base, blogs and guides to provide regular updates on emerging threats, and quick access to IT support. This keeps them informed and equipped to act when new cyber challenges arise.

Step 3: Monitoring and continuous improvement

Keep an eye on how well your training programme is working by tracking key metrics. Use quizzes, surveys, and simulated phishing results to see how much employees are learning and progressing.

Look at things like phishing email click rates, quiz scores, and the number of reported security incidents. Regularly ask employees for feedback to understand their experiences and challenges and adjust as needed.

Since cyber threats are always changing, your training programme should too. Update the content regularly to reflect new threats, technologies, and best practices. Stay informed about the latest in cyber security and adjust your training accordingly.

Finally, recognise and reward employees who excel in cyber security practices. Positive reinforcement can motivate others to take the training seriously and strive for better performance.

www.pisys.net

Types of cyber awareness training

Not all training methods are created equal, and choosing the right approach can make a big difference in how well your employees absorb and apply the knowledge.

There are two main styles of training: Traditional and interactive.

Traditional training methods

Classroom-based training is an instructor-led session where employees gather to learn about cyber security. It can cover complex topics in a structured way, offering face-to-face interaction with an expert. However, this format often lacks engagement and may not always hold employees' attention.

PROS

Direct interaction with a knowledgeable instructor and the chance for real-time Q&A.

CONS

Can feel monotonous, making retention difficult. It's also time-consuming and may disrupt the workday.

Online courses and webinars provide flexibility, allowing employees to learn at their own pace. These can be live sessions or pre-recorded modules that cover various aspects of cyber security training, from phishing awareness to data protection.

PROS

Employees can schedule training around their work, and there is a wide range of topics available.

CONS

These sessions can be passive, with a risk of distractions. Without hands-on activities, it's harder to stay engaged.

Interactive training methods

Interactive training actively engages employees, making the learning process more memorable and applicable. It goes beyond just listening and reading, ensuring your team is ready to recognise and respond to threats.

Phishing simulations are a powerful way to test your employees' ability to identify and react to phishing attacks. These simulated attacks are sent out as real phishing attempts would be, and the results can help highlight gaps in awareness and training. When combined with regular cyber security training, phishing simulations ensure that employees stay sharp and vigilant.

PROS

Realistic, hands-on experience that directly addresses a common attack method.

CONS

Can cause anxiety if not communicated properly and managed sensitively.

Gamified training uses game elements like quizzes, leaderboards and rewards. This approach makes cyber security training fun and competitive, which helps boost engagement and retention. Employees are more likely to absorb key lessons when they're motivated by challenges and rewards.

PROS

Highly engaging, with increased retention through repetition and competition.

CONS

Developing gamified content can require more time and resources.

Role-playing scenarios place employees in hypothetical cyber-attack situations. They need to respond as they would in real life, practicing decision-making under pressure. This hands-on approach is excellent for reinforcing how to handle phishing emails, ransomware threats, or security breaches.

PROS

Offers practical experience and encourages critical thinking.

CONS

Some employees might not take it seriously or feel uncomfortable with the pressure.

Interactive workshops combine traditional instruction with practical exercises. These workshops might include group discussions, real-world case studies, and collaborative problem-solving activities. They offer a well-rounded learning experience by mixing theory with practice.

PROS

A balanced approach with opportunities for collaboration and peer learning.

CONS

Requires careful planning and skilled facilitators, and can be time-consuming.

Interactive cyber security training is an excellent way to keep employees engaged and eager to learn. Simulations provide hands-on experience, helping staff apply their new knowledge to real-world situations. For example, simulated phishing attacks offer immediate feedback, allowing employees to learn from mistakes in a controlled environment.

Adding gamified elements, like quizzes and friendly competition, can make the training fun and motivate employees to improve their skills. This type of active participation leads to better retention and a deeper understanding of key cyber security concepts. It transforms training from a passive exercise into an engaging, practical experience.

Striking a Balance in Cyber Security Training

While interactive methods are highly effective, a balanced approach that incorporates both traditional and interactive styles is often the most beneficial. Combining foundational learning through online courses with hands-on activities like phishing simulations ensures employees have both the theoretical knowledge and practical skills they need to defend against cyber threats.

For instance, at NumberCrunch, they implemented a balanced training programme that included regular online modules for core knowledge, supplemented by quarterly interactive workshops and phishing simulations. This approach ensured staff not only understood the basics but also had the opportunity to apply their learning in real-world scenarios.

Comprehensive Cyber Security Training with Pisys

At Pisys, we provide cyber security training options through our eCampus platform. Whether your business requires the flexibility of online courses or the immersive experience of phishing simulations, we can tailor a training programme to meet your specific needs. Our training is designed to engage employees, improve retention and reinforce best practices, ensuring your team stays ahead of the latest threats.

Building a Cyber Security Culture

Creating a strong cyber security culture is essential for protecting your business from ever-evolving threats. This involves embedding security into every aspect of your operations and making it part of your employees' daily behaviour. When cyber security becomes second nature, your organisation will be far better equipped to prevent attacks and mitigate risks.

Leadership Sets the Tone

Cyber security starts at the top. Leadership needs to actively participate in cyber security training and champion security initiatives across the business. When senior managers take cyber security seriously, it sets a powerful example for the rest of the company. Sharing personal experiences and consistently communicating the importance of security can help reinforce this message.

Investing in cyber security resources, such as specialised training programmes and skilled IT partners, demonstrates a clear commitment to safeguarding the business. It shows that you are serious about protecting company data, client information, and overall operations from cyber threats.

Empower Employees

It’s crucial to empower every employee to take responsibility for cyber security. When staff feel ownership over their role in keeping the business secure, they are more likely to be proactive. Encourage them to report suspicious activity and remain alert to potential threats. Keep security at the forefront of everyone’s mind with regular updates, newsletters, and company-wide meetings.

Creating an open environment where employees feel comfortable discussing cyber security concerns is equally important. Provide clear reporting channels and ensure there’s no fear of blame for raising an issue. Promoting collaboration across departments can also foster new ideas for strengthening your security posture.

Reinforce Good Habits

Maintaining a strong cyber security culture requires regular reinforcement. Weekly security tips, periodic refresher training, and visible reminders around the office can help keep employees engaged with best practices. Recognition also plays a key role. Publicly acknowledge employees who excel in cyber security awareness, whether through awards, small incentives, or even a simple "thank you." Positive reinforcement can motivate others to improve their behaviour and contribute to a security-first environment.

A Continuous Journey

Building a cyber security culture is not a one-time task; it’s an ongoing effort that evolves alongside new threats and technology. However, it doesn’t have to be overwhelming. With a clear strategy in place—supported by regular training, employee engagement, and leadership commitment—you can foster a secure and resilient organisation.

Building a cyber security culture

Cyber security is a continuous journey that takes commitment, but it doesn't have to become a headache.

At Pisys, we make this journey easier. We can help you develop and implement a tailored cyber security programme, from planning to cyber security training and even cultural change. Contact Pisys to learn more about how we can support your business in building a strong, security-focused culture.

This is something we help businesses like yours with all the time. If we can help you in 2024,

Get in touch.

CALL: 01792 464748
EMAIL: hello@pisys.net
WEBSITE: www.pisys.net

PISYS .net
A COMCEN COMPANY