UNDERSTANDING

CYBERSECURITY AWARENESS

Your Staff Is Often Your Last Line Of Defense

An Informational eBook

CORE6+

Visit https://Core6Plus.com to learn more.

UNDERSTANDING

CYBERSECURITY AWARENESS

Your Staff Is Often Your Last Line Of Defense

An Informational eBook

Table of Contents: CyberSecurity Awareness Training

Chapter 1: The Human Element

1.1 The Security Gap: Why Human Error is the Leading Cause of Breaches

The most sophisticated firewalls and advanced security systems in the world can only do so much. The reality is that the single biggest security gap in any organization's defense is not its technology, but its people. In fact, studies show that nearly

95% of all data breaches are caused by human error.

Think about this:

90% of all breaches start with just one careless click. Phishing emails alone accounted for almost 90% of all data breaches in 2023. These aren't technical failures; they're human mistakes, born from a lack of awareness and vigilance. Without proper training, your investment in technology could be easily undone by one untrained click.

1.2 You Are a Target: The Reality of Opportunistic Attacks

Many business owners fall into the trap of believing they are "too small" or "too insignificant" to be targeted by hackers. This belief is not just naive; it's **absolutely wrong**. Most cyber crimes are not targeted; they are **opportunistic**.

Hackers don't wake up and decide to specifically attack your business. Instead, they launch automated attacks in volume against "purchased" lists of email addresses, looking for any open door they can find. The data shows that small businesses are the largest target for these opportunistic attacks because a large percentage of them do not invest in appropriate awareness training or protection. The simple lack of awareness and "true" protection makes small to medium-sized businesses the perfect target.

1.3 The Cost of Cyber Complacency: What Happens When You Don't Take It Seriously

The worst thing anyone can do is to be complacent with a "that'll never happen to me" kind of attitude. This mindset of

"cyber complacency" leads to poor, if not horribly unfortunate, decisions that have real and painful repercussions for businesses of any size.

A single simple error can lead to serious damage for both the individual and the company. The cost of a security breach has never been higher, with the global average cost reaching $4.45M in 2023. This isn't just about financial loss; it's about losing customer trust and a damaged reputation. The risk of a cyber attack for every company of any size is very real and should be deemed too great to ignore.

Chapter 2: The Solution - A Complete Training Program

2.1 What is Core 6+ Training? A Proactive Defense for Your Team

If human error is the security gap, then **Core 6+ CyberSecurity Awareness Training** is the proactive defense that closes it. Our training is a comprehensive program designed to educate your entire team and to build a strong, security-minded culture within your organization.

This solution is more than just a course; it’s a strategic defense that recognizes that your employees are both your first and last line of defense against cyber threats. It empowers them with the knowledge and the tools to recognize, avoid, and report cyber attacks, transforming your company's biggest vulnerability into a powerful line of protection.

2.2 The Basics: A Web-Based, Self-Paced Course

The foundation of our training program is a web-based, self-paced course that is designed to be engaging and informative. All of your staff will gain access to our CyberSecurity Awareness Training Portal, where they will go through multiple training segments with a "mini-quiz" after each segment. This ensures that staff understand what is required of them and have the skills required to identify a cyber attack.

The course is designed to be completed at their own pace, and when each of your employees has completed the training, they will get a certificate of completion for that year of training. We highly recommend that each of your employees go through the annually updated training every year.

Visit https://Core6Plus.com to learn more.

2.3 Beyond a One-Time Event: The Power of Weekly Micro-Training

A single annual training session is not enough to keep your team prepared against an ever-evolving threat landscape. Cyber criminals continually evolve, and your defense strategy should evolve with it. **Weekly Micro-Training** is one of the best ways to fortify your front-line defense.

Core 6+ provides weekly CyberSecurity Awareness "refreshers" to help maintain vigilance. Once your employees have completed the annual training, we will move them into a weekly email campaign, where they will receive an email that identifies a new variant of concern/attack and helps each person maintain a security-minded vigilance. This consistent reinforcement empowers employees to protect themselves, clients, and the business, recognizing that staying alert and on-guard is an everyday event.

Chapter 3: The Benefits of a Trained Team

3.1 A Human Firewall: Turning Your Weakest Links into Your Greatest Strength

While employees can be a company's greatest vulnerability, they are also its greatest defense. A cybersecurity awareness program can turn your "weakest links" into your "greatest strengths". It empowers employees to take an active role in protecting the company's digital assets.

Training helps reduce the risk of security incidents by teaching employees to recognize and avoid cyber threats. It teaches them to spot phishing emails and understand the dangers of social engineering attacks. With proper education, your team becomes a "human firewall," capable of proactively identifying and stopping threats before they can compromise your network.

3.2 A Culture of Security: Building Vigilance into Your Daily Operations

A strong security culture is a critical component of any comprehensive security plan. It’s about more than just a training program; it’s about fostering a climate of accountability where every team member understands their role in maintaining security.

Training helps to build this culture by making security a daily operational habit, not just a checklist item. When employees feel empowered with the knowledge and confidence to handle security threats, they are more likely to adhere to policies and report suspicious activities. This creates a more knowledgeable and watchful workforce, which lowers the possibility of security issues and improves incident response times.

Visit https://Core6Plus.com to learn more.

3.3 The Ultimate Advantage: How Training Protects Your Business

The ultimate advantage of a trained team is how it protects your business from the significant financial, operational, and reputational damage of a breach.

- **Cost-Efficiency:** Training helps to minimize the risk of financial losses associated with data breaches, including fines, lost business, and damage to the organization's reputation.
- **Compliance:** Many industries are subject to strict data protection regulations and standards. Training ensures that employees are aware of and can adhere to these regulations, helping to avoid legal penalties.
- **Customer Trust:** Enhancing customer confidence and trust in the business’s ability to protect their personal information is crucial for maintaining a good reputation. A well-informed and vigilant workforce can lead to fewer security incidents and can also help to lower insurance premiums by demonstrating a proactive approach to risk management.

Table of Contents: CyberSecurity Awareness Training

Here is the complete eBook on Cybersecurity Awareness Training, following the approved outline.

Chapter 1: The Human Element

1.1 The Security Gap: Why Human Error is the Leading Cause of Breaches

The most sophisticated firewalls and advanced security systems in the world can only do so much. The reality is that the single biggest security gap in any organization's defense is not its technology, but its people. In fact, studies show that nearly

95% of all data breaches are caused by human error.

Think about this:

90% of all breaches start with just one careless click. Phishing emails alone accounted for almost

90% of all data breaches in 2023. These aren't technical failures; they're human mistakes, born from a lack of awareness and vigilance. Without proper training, your investment in technology could be easily undone by one untrained click.

1.2 You Are a Target: The Reality of Opportunistic Attacks

Many business owners fall into the trap of believing they are "too small" or "too insignificant" to be targeted by hackers. This belief is not just naive; it's

absolutely wrong. Most cyber crimes are not targeted; they are

opportunistic.

Hackers don't wake up and decide to specifically attack your business. Instead, they launch automated attacks in volume against "purchased" lists of email addresses, looking for any open door they can find. The data shows that small businesses are the largest target for these opportunistic attacks because a large percentage of them do not invest in appropriate awareness training or protection. The simple lack of awareness and "true" protection makes small to medium-sized businesses the perfect target.

1.3 The Cost of Cyber Complacency: What Happens When You Don't Take It Seriously

The worst thing anyone can do is to be complacent with a "that'll never happen to me" kind of attitude. This mindset of

"cyber complacency" leads to poor, if not horribly unfortunate, decisions that have real and painful repercussions for businesses of any size.

A single simple error can lead to serious damage for both the individual and the company, who must report the incident to the appropriate regulators as well as their customers. The cost of a security breach has never been higher, with the global average cost reaching

$4.45M in 2023. This isn't just about financial loss; it's about losing customer trust and a damaged reputation. The risk of a cyber attack for every company of any size is very real and should be deemed too great to ignore.

Chapter 2: The Solution - A Complete Training Program

2.1 What is Core 6+ Training? A Proactive Defense for Your Team

If human error is the security gap, then

Core 6+ CyberSecurity Awareness Training is the proactive defense that closes it. Our training is a comprehensive program designed to educate your entire team and to build a strong, security-minded culture within your organization.

This solution is more than just a course; it’s a strategic defense that recognizes that your employees are both your first and last line of defense against cyber threats. It empowers them with the knowledge and the tools to recognize, avoid, and report cyber attacks, transforming your company's biggest vulnerability into a powerful line of protection.

2.2 The Basics: A Web-Based, Self-Paced Course

The foundation of our training program is a web-based, self-paced course that is designed to be engaging and informative. All of your staff will gain access to our CyberSecurity Awareness Training Portal , where they will go through multiple training segments with a "mini-quiz" after each segment. This ensures that staff understand what is required of them and have the skills required to identify a cyber attack.

The course is designed to be completed at their own pace, and when each of your employees has completed the training, they will get a certificate of completion for that year of training. We highly recommend that each of your employees go through the annually updated training every year.

Visit https://Core6Plus.com to learn more.

2.3 Beyond a One-Time Event: The Power of Weekly Micro-Training

A single annual training session is not enough to keep your team prepared against an ever-evolving threat landscape. Cyber criminals continually evolve, and your defense strategy should evolve with it.

Weekly Micro-Training is one of the best ways to fortify your front-line defense.

Core 6+ provides weekly CyberSecurity Awareness "refreshers" to help maintain vigilance. Once your employees have completed the annual training, we will move them into a weekly email campaign, where they will receive an email that identifies a new variant of concern/attack and helps each person maintain a security-minded vigilance. This consistent reinforcement empowers employees to protect themselves, clients, and the business, recognizing that staying alert and on-guard is an everyday event.

Chapter 3: The Benefits of a Trained Team

3.1 A Human Firewall: Turning Your Weakest Links into Your Greatest Strength

While employees can be a company's greatest vulnerability, they are also its greatest defense. A cybersecurity awareness program can turn your "weakest links" into your "greatest strengths". It empowers employees to take an active role in protecting the company’s digital assets.

Training helps reduce the risk of security incidents by teaching employees to recognize and avoid cyber threats, which significantly reduces the risk of security breaches. It teaches them to spot phishing emails and understand the dangers of social engineering attacks, and to maintain a vigilant stance against all types of cyber attacks.

3.2 A Culture of Security: Building Vigilance into Your Daily Operations

A strong security culture is a critical component of any comprehensive security plan. It’s about more than just a training program; it’s about fostering a culture of security where every team member understands their role in maintaining security.

Training helps to build this culture by making security a daily operational habit, not just a checklist item. When employees feel empowered with the knowledge and confidence to handle security threats, they are more likely to adhere to policies and report suspicious activities, which enhances the company's security posture. This continuous reinforcement acts as a continuous reminder that security is everyone’s responsibility, reinforcing best practices across the organization.

3.3 The Ultimate Advantage: How Training Protects Your Business

The ultimate advantage of a trained team is how it protects your business from the significant financial, operational, and reputational damage of a breach.

- **Cost-Efficiency:** Training helps to minimize the risk of financial losses associated with data breaches, including fines, lost business, and damage to the organization's reputation.
- **Compliance:** Many industries are subject to strict data protection regulations and standards. Training ensures that employees are aware of and can adhere to these regulations, helping to avoid legal penalties.
- **Customer Trust:** Enhancing customer confidence and trust in the business’s ability to protect their personal information is crucial for maintaining a good reputation. A well-informed and vigilant workforce can lead to fewer security incidents and can also help to lower insurance premiums by demonstrating a proactive approach to risk management.

Chapter 4: The Conclusion

4.1 A Summary of What Matters Most

We've explored the world of cybersecurity, moving from the dangers of the inbox to the peace of mind of a proactive defense. As we bring this guide to a close, let's quickly recap the most important takeaways:

1. **The Human Element is the Key:** Human error is the single biggest cause of data breaches , and training is the single biggest factor in preventing successful attacks.
2. **You Are a Target:** Most cyber crimes are not specific; they are opportunistic, and small businesses are the perfect target due to a lack of awareness and protection.
3. **Training is a Complete Program:** It's a web-based, self-paced course with a certificate of completion, and it is reinforced by weekly micro-training refreshers to maintain vigilance.
4. **Your Employees are Your Human Firewall:** Training empowers employees to take an active role in protecting the company's digital assets, turning them into a proactive defense that closes the security gap.

Visit https://Core6Plus.com to learn more.

4.2 The Peace of Mind: A Final Look at the Ultimate Benefit

The ultimate benefit of a robust training program is the peace of mind that comes with knowing your team is prepared. As a business owner or a nonprofit director, you shouldn't have to worry that a single careless click will lead to a catastrophic shutdown.

With a comprehensive training program, you can operate with the confidence that a team of experts is constantly on guard. You have a partner who is proactively working to prevent a single careless click from turning into a major disruption. You can focus on what you do best: running your business and making a difference in your community.

Visit https://Core6Plus.com to learn more.

4.3 The Final Statement

Transform Your Security From Passive Recording, To An Active, Intelligent, Real-Time Managed Solution!

Visit https://Core6Plus.com to learn more.

Your Strategic CyberSecurity Provider (SCP)

Core 6+ is your Strategic CyberSecurity Provider (SCP) — a partner focused exclusively on protecting your organization from today's ever-evolving cyber threats. Unlike traditional MSPs that primarily handle IT labor and computer fixes, Core 6+ delivers the world's best, proactive cybersecurity protection applications and defense tools through layered solutions like Gateway Protection, SOC-managed EDR, NOC-managed Daily Patching and Preventative Maintenance, Web Protection and DNS Filtering, Data Backups, and more. Core 6+ augments and works directly with your trusted IT support – whether that be internal staff or external contractor. Core 6+ wants to help augment your team by providing 24/7 real-time, all-the-time protection, Where You Want It Most — giving you the freedom to choose only what you need, at a price you can actually afford.

Traditional MSPs tend to - and often want to - live on one end of the service spectrum with fully "Done For You" services option, which always include high fees and retainers. Whereas, at the other end of that spectrum, where most small businesses and nonprofits are, the only option for cybersecurity protection seems to be: (Pay Way Too Much, or) "Do It Yourself" - literally leaving small businesses and nonprofits on their own, with no professional guidance, and with no real safety net.

Core 6+, as your SCP, bridges that gap. Giving organizations - of every size - the freedom to handle as much of their own IT and computer support as they want and have been doing for years. Core 6+ works with whoever your trusted IT support person is… And, if need be, Core 6+ can help you find local IT Partners to provide complete, hands-on service when needed.

With Core 6+, as your SCP, partnering with your trusted IT support you can get the perfect blend of CyberSecurity Protection, IT independence and the expert (augmented) backup support if, or whenever needed.