ISSUE 018
January 2025
Independence, Missouri

FCS TECH TALK

Your Trusted Technology Partner Since 1989

INSIDE THIS ISSUE:

SECURITY AWARENESS TRAINING AND PHISHING CAMPAIGNS: IMPORTANCE AND BENEFITS

In today's digital age, cyber security is no longer a concern limited to large corporations. Small businesses, often considered the backbone of the economy, are increasingly becoming prime targets for cybercriminals.

Small Business Attacks

According to a report by the U.S. Small Business Administration, nearly half of all cyberattacks are directed at small businesses. Despite this, many small business owners underestimate the importance of robust cyber security measures. One of the most effective ways cybercriminals are attacking small businesses is through Phishing attacks.

Phishing has become a dominant method in the arsenal of cybercriminals, responsible for the majority of cyber incidents. According to the Cybersecurity and Infrastructure Security Agency (CISA), over 90% of successful cyberattacks begin with a phishing email.

Phishing attacks typically involve cybercriminals masquerading as trusted entities to deceive individuals into sharing sensitive information, such as login credentials, financial details, or personal data. These attacks are not only prevalent but also increasingly sophisticated, making them difficult to detect without proper training.

Why Phishing Is So Effective

Exploitation of Human Error: Phishing targets the human tendency to trust. Even well-educated employees can fall victim to cleverly disguised emails.

Rapid Adaptation: Cybercriminals continually refine their tactics, using advanced techniques like spear-phishing and fake websites to appear legitimate.

Wide Reach: Phishing attacks are cost-effective and scalable, enabling attackers to target numerous victims simultaneously.

How can Small Businesses Combat Phishing?

One of the most effective ways to combat phishing attacks and to mitigate risks for small businesses is through the use of security awareness training and phishing campaigns.

Why Security Awareness Training is Essential

Security awareness training involves educating employees about potential cyber security threats, teaching them how to recognize and respond to risks effectively.

For small businesses, this type of training is crucial for several reasons:

Humans Are the Weakest Link: Even the most sophisticated security infrastructure can be compromised by human error. A single click on a malicious link can expose an organization to malware, ransomware, or data breaches.

Cost-Effective Risk Mitigation: Investing in security awareness training is often far more affordable than dealing with the aftermath of a cyberattack. The costs of data recovery, legal fees, and reputational damage can be devastating for small businesses.

Regulatory Compliance: Many industries have regulatory requirements for data protection, such as GDPR, HIPAA, and PCI-DSS. Training ensures employees adhere to these standards and reduces the risk of costly non-compliance penalties.

Building a Security Culture: Training fosters a culture of cyber security within the organization, encouraging employees to prioritize safety and vigilance in their daily activities such as, taking the time to double check an email address before replying to an email or rereading a new email from a first-time sender to make sure that it is not a phishing attack.

Understanding Phishing Campaigns

Phishing campaigns are simulated cyberattacks designed to test employees' ability to recognize and avoid fraudulent communications. These exercises are a critical component of any comprehensive security awareness program. Here's why:

Real-World Training: Simulated phishing campaigns provide hands-on experience, enabling employees to practice identifying and responding to threats in a controlled environment.

Identifying Vulnerabilities: These exercises reveal gaps in knowledge and areas where employees may require additional training.

Continuous Improvement: Regular phishing simulations help businesses track progress and adapt their training programs based on employee performance.

Boosting Confidence: By practicing how to handle potential threats, employees gain confidence in their ability to respond appropriately, reducing panic and mistakes during actual incidents.

Benefits of Security Awareness Training and Phishing Campaigns

Reduced Risk of Cyberattacks: Employees who can recognize phishing emails, suspicious links, and other threats are less likely to fall victim to attacks, significantly reducing the likelihood of a security breach.

Cost Savings: Preventing cyberattacks saves businesses money by avoiding costs associated with data breaches, downtime, and lost customer trust.

Improved Employee Morale: Employees feel empowered and valued when they are equipped with the knowledge and tools to protect themselves and the company.

Strengthened Customer Trust: Customers are more likely to do business with companies that demonstrate a commitment to cyber security, enhancing the organization's reputation and customer loyalty.

Compliance and Legal Protection: Many cyber security regulations require businesses to implement employee training. Meeting these standards can protect the business from legal repercussions and fines.

For small businesses, investing in security awareness training and phishing campaigns is not just a best practice—it's a necessity. These programs provide a cost-effective way to reduce the likelihood of a cyberattack and ensure that employees are well-prepared to act as a robust line of defense.

By fostering a culture of security awareness and combining it with technical safeguards, small businesses can protect their operations, customers, and reputations in an increasingly digital world. Failing to prioritize cybersecurity could mean the difference between thriving in the modern market and falling victim to costly and avoidable breaches.

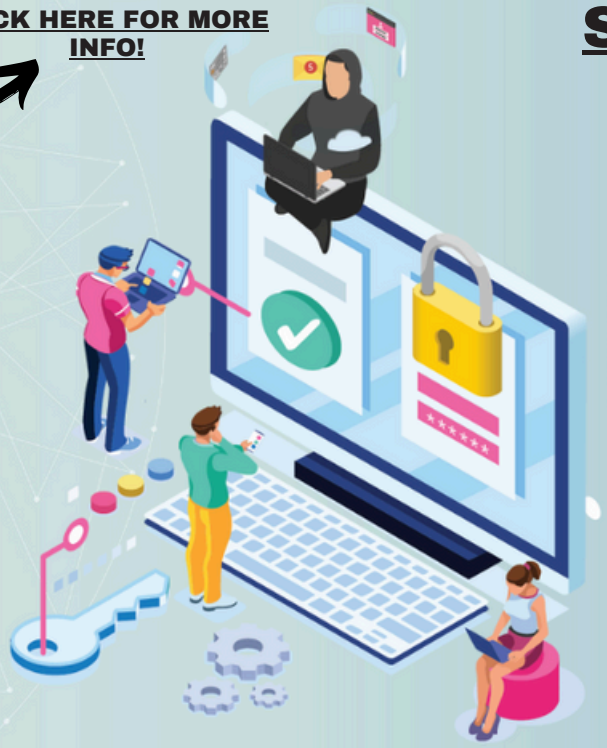
FCS can help provide all the tools needed for your small business to start getting Security Awareness Training and Phishing Campaigns. We have seen firsthand how effective this training can be. Now before clicking a link on an email or replying to an email address that seems to be misspelled, employees and collogues are more likely to scrutinize these emails and raise awareness to the risks involved with opening emails thanks to Security Awareness Trainings.

With training and awareness, phishing threats can be dramatically decreased and small businesses can stay protected.

ISSUE 018
January 2025
Independence, Missouri

THIS MONTH'S PRODUCT SPOTLIGHT

CLICK HERE FOR MORE INFO!



SECURITY AWARENESS TRAINING

- **Engaging Monthly Video Training**
- **Relevant Topics to Real World Threats**
- **Quick and Easy to Follow Material**

HOW AI CAN HELP IMPROVE YOUR WORK

Artificial Intelligence (AI) has transformed the way we work, offering tools and solutions to simplify tasks, boost productivity, and improve focus.

Here are some practical ways AI can assist you while working at your computer:

1. Automating Repetitive Tasks

AI-powered tools like Zapier and Microsoft Power Automate can handle routine tasks such as sorting emails, organizing files, or generating reports.

By automating these time-consuming activities, you can focus on high-priority work that requires your expertise.

2. Enhancing Writing and Communication

Tools like Grammarly and QuillBot provide real-time grammar corrections, suggestions for clarity, and tone adjustments.

AI also aids in generating professional emails, reports, or presentations, ensuring your communication is polished and effective.

4. Improving Focus

AI apps like RescueTime track your work habits and provide insights into how you spend your time.

Tools like Freedom or Serene use AI to block distracting websites and create customized focus sessions, helping you stay on task.

5. Streamlining Research

AI tools like ChatGPT or Elicit help with gathering information quickly and summarizing complex topics.

They can assist with brainstorming, drafting ideas, and even answering specific queries, making them valuable for content creation and research tasks.

6. Optimizing Workflows

AI in project management tools like Monday.com, Trello, or Notion helps analyze workflows, predict deadlines, and identify bottlenecks.

These insights enable teams to allocate resources effectively and meet goals more efficiently.

7. Managing Data and Insights

AI excels at processing large amounts of data. Tools like Tableau and Power BI use AI to generate visual reports and uncover patterns in your data, making it easier to make informed decisions.

BEST PRACTICES FOR SECURE DATA BACKUP

Data backup refers to the creation of a copy of your data. The copy can be used in the event of loss or destruction of the original data.

Backups can be stored on various devices, such as external hard drives, or in the cloud. Having a backup ensures you don't lose important information.

Here are best practices for secure data backup:

• **Use Encryption:**
Encryption scrambles your data so only you can read it. This keeps it safe from hackers.

• **Set Strong Passwords:**
Use strong passwords for all your backup accounts and devices. This prevents unauthorized access.

• **Regularly Test Your Backups:**
Testing ensures that your backups work properly. Try restoring a file to make sure everything is correct.

Take Action to Protect Your Data Today

Don't wait until it's too late to protect your data. Start backing up today!

Secure your important files by following these best practices for data backup. FCS can help with all of your backup needs making sure your data stays safe and secure!

DESKTOP VS LAPTOP: THE PROS AND CONS

In today's fast-paced digital world, deciding whether to invest in a desktop or a laptop can be a tricky decision. Both devices have their own strengths and weaknesses, and the best choice often depends on your lifestyle, work habits, and personal preferences. Let's break down the pros and cons of desktops and laptops, and explore how to make the right decision for your needs.

Pros and Cons of Desktops: Pros

More Power for Less Money: Desktops generally offer more power than laptops at a similar price point. With room for larger components like graphics cards, faster processors, and better cooling systems, desktops can handle heavy-duty tasks like gaming, video editing, and 3D rendering more effectively.

Upgradeability: One of the biggest advantages of a desktop is its flexibility for upgrades. If you find that your system is starting to lag, you can swap out individual parts like RAM, storage, or even the graphics card to keep your machine up-to-date.

Better Ergonomics: Desktops allow for a more comfortable and customizable work setup. With a larger screen, separate keyboard, and adjustable chair, you can create an ergonomic workspace that helps prevent strain or injury from prolonged use.

Longer Lifespan: Since desktops are easier to maintain and upgrade, they can last longer than laptops. Many desktops also tend to have a better cooling system, reducing the risk of overheating and prolonging the life of internal components.

Pros and Cons of Desktops: Cons

Lack of Portability: Desktops are stationary. Once you set them up in your home or office, they aren't easy to move around. If you need to work on-the-go or take your computer to different locations, a desktop isn't the best option.

Takes Up More Space: Desktops require a desk or a dedicated space. Along with the tower, you'll need room for a monitor, keyboard, and mouse, which can contribute to clutter if your workspace is limited.

More Cables: With separate components, desktops can lead to a mess of cables. Keeping everything organized can be challenging, especially if you're working with multiple monitors or peripheral devices.

Pros and Cons of Laptops: Pros

Portability: The major selling point of laptops is their portability. Whether you need to work in a café, move from one office to another, or take your work on vacation, laptops offer convenience. Their compact nature means you can easily throw one into a bag and go.

Space-Saving: Laptops combine all necessary components (monitor, keyboard, trackpad) into a single unit, so they require less desk space. If you have a small workspace or need to travel light, a laptop is the way to go.

Less Cable Clutter: Unlike desktops, laptops are self-contained. You only need a power cable to plug into an outlet, and some laptops even offer wireless charging and Bluetooth, reducing the need for additional cords and cables.

Integrated Features: Laptops come with built-in features like webcams, speakers, and microphones, making them ideal for remote meetings, video calls, or streaming media without the need for external peripherals.

Pros and Cons of Laptops: Cons

Limited Power and Upgradeability: Laptops can't match the raw power of a desktop. While high-end models can handle most tasks, they're still limited by their compact design and inability to be easily upgraded. If your laptop starts to slow down or if you need more storage or better performance, you often have to replace the whole device.

Smaller Screen Size: Laptops typically come with smaller screens than desktop monitors, which can be a drawback if you prefer to work with multiple windows open at once or need extra screen real estate for productivity or design tasks.

Higher Cost for Comparable Performance: Laptops are often more expensive than desktops with similar specs. Because of their compact design, laptops require specialized parts, which can drive up the price, especially when it comes to premium models with powerful processors and graphics cards.

Shorter Lifespan: Due to their small size, laptops have less room for cooling systems, which can lead to overheating if they're used extensively for demanding tasks. In general, laptops also don't last as long as desktops due to their non-upgradable nature and limited repairability.

Desktop or Laptop: Which should you choose?

Ultimately, the choice between a desktop and a laptop depends on your specific use case. Desktops are ideal for those seeking power, performance, and upgradeability, while laptops shine in portability and convenience.

Take some time to assess your needs, workspace, and budget to determine which option will serve you best. FCS can help you decide which device will be the best fit for you helping you increase productivity while not breaking the bank to do so!

ISSUE 018
January 2025
Independence, Missouri

ULTIMATE GUIDE TO ENCRYPTION METHODS

Encryption is a method of securing information. It converts readable data into secret code. Only the right key can decode it. This guide will help you understand different encryption methods.

What is Encryption?

Encryption is like a secret language. It converts regular text into unreadable text. This unreadable text is called ciphertext. Only people who have the right key will be able to convert it into normal text, called plaintext.

Why Do We Use Encryption?

We use encryption to keep our information safe. It makes our data safe from hackers. This is very important for privacy and security.

How Does Encryption Work?

Encryption uses algorithms and keys. An algorithm is a set of rules for solving problems. A key is somewhat like a password that unlocks the secret message.

Symmetric vs Asymmetric Encryption

Symmetric encryption uses the same key for encryption and decryption. The same key is shared between the sender and receiver. It's fast but less secure when the key is shared.

Asymmetric encryption uses two keys: a public key and a private key. A public key can encrypt a message, while a private key can decrypt it. It's more secure since only the private key unlocks the message.

What Are Some Common Encryption Methods

- AES (Advanced Encryption Standard)
- RSA (Rivest-Shamir-Adleman)
- DES (Data Encryption Standard)
- ECC (Elliptic Curve Cryptography)

How Do We Use Encryption in Everyday Life?

- Online Shopping. When you purchase online, your payment information is encrypted. This protects your credit card information against hackers.
- Messaging Apps. Apps like WhatsApp use encryption to keep your messages private. Only you and the person you are chatting with can read them.
- Email Security. Many email services use encryption to protect your emails from being read by others.

How Can You Stay Safe with Encryption?

- Use Strong Passwords. Always use strong passwords for accounts and devices. That will make hacking difficult as it will take time to access.
- Keep Software Up-to-Date. Regularly update your software to protect against security vulnerabilities in software.
- Use Caution with Public Wi-Fi. If you need to use public Wi-Fi, avoid sensitive transactions unless you can encrypt your internet connection using a VPN.

Ready to Secure Your Data?

Encryption helps protect your personal information from threats. Understanding different methods can help you choose the right one for your needs.

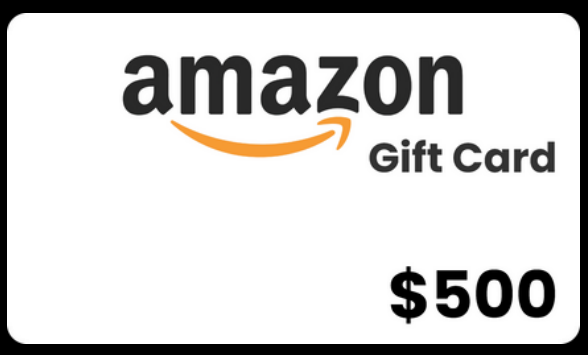
If you need help securing your data, contact us today! We can make sure that all of your important data is safely stored and secured through encrypted backups.

WE LOVE REFERRALS

The greatest gift anyone can give us is a referral to another business in need of IT services. Referrals help us keep costs down so we can pass the savings to our clients.

If your referral ends up becoming a client - we'll gift them their first month of service at no charge AND we'll gift you a $500 Amazon Gift Voucher.

Simply introduce me via email to stan@fcskc.com and I'll take it from there. I personally promise we'll look after your referral's business with a high level of care and attention (just like we do with all our clients).
-Stan



We Want Your Feedback

Here at Ferguson Computer Services, we value your feedback greatly and would appreciate if you took time from your busy schedule to leave us a review. These reviews let us know what we are doing well and what we might be able to improve on in the future.

Leave a Google Review Leave a Facebook Review

TECHNOLOGY TRIVIA TIME

Technology Trivia Question of the Month! Send the correct answer to winner@fcskc.com to be entered to win a $50 gift card to Amazon.

Here is January's question of the month: What percent of successful cyberattacks start with a Phishing email?