1991 – 2021
30 YEARS OF EXCELLENCE
Computer Technologies, Inc.

TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's Inside

Security Awareness Training: The Key to Securing Home And Networks ……Page 1

FREE: Dark Web Scan……Page 2

Security Corner: Are Your Social Media Profiles Secure? ……Page 3

Guide To Secure File Storage And File Transfers ……Page 3

How To Minimize Ransomware Damage ……Page 4

8 Ways To Organize Your Devices For Productivity ……Page 4

March 2025

Kim Nielsen, CISSP, CCSA
President & Chief Technology Strategist at Computer Technologies Inc.
(248) 362-3800

"As a business owner, you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

Security Awareness Training: The Key to Securing Home and Work Networks

In today's digital age, cybersecurity is more critical than ever. We interact with people online all the time, for work and in our personal life. This constant digital connection makes us vulnerable to various cybersecurity threats.

That's what makes Security Awareness Training so important. These informational courses, which you take ideally every month but at least every year at your job, update you about the latest cybersecurity statistics and defensive tactics that best protect your systems and data from all of the threats plaguing SMBs like your own. We recommend taking it every month because cybersecurity and cyber-threats are constantly changing, and we need to update our own awareness on a regular basis to keep up.

What is Security Awareness Training?

Your cybersecurity training is a structured program designed to educate employees just like you about the various cybersecurity threats you might encounter and the best practices to defend against them. This training typically covers topics such as:

- Phishing and Social Engineering: Recognizing and avoiding deceptive emails and messages.
- Password Management Creating and maintaining strong, unique passwords.
- Data Protection: Safeguarding sensitive information from unauthorized access.
- Safe Internet Practices: Navigating the web securely and avoiding malicious sites.

Continued on pg.2

Continued from pg.1

- Incident Reporting: Knowing how to report suspicious activities or breaches.

Cybersecurity is a constantly evolving field. New threats emerge daily, and attackers continuously develop more sophisticated methods to breach defenses. Security training ensures that employees are aware of the latest tactics used by cybercriminals. It also helps reinforce good cybersecurity practices, making them second nature so you can respond immediately to suspicious activity.

On top of the security training provided by your job, it's also best to refresh your knowledge more often than that. How well do you remember something you cover once per month or year? Not as well as you'd remember tips that you go over once per week, or even daily!

Follow cybersecurity hashtags and news, keep your systems updated with the latest security tools available, and make use of the weekly Security Short videos and other resources that we provide for you!

How It Helps Secure Our Home and Work Networks

Effective security awareness training has a ripple effect, enhancing security both at work and at home. How does it affect your digital life in so many different ways.

Firstly, trained employees are more likely to recognize and avoid potential threats. This increased vigilance greatly reduces the risk of a breach. Employees who understand the best practices, like the importance of strong passwords, are less likely to use weak or reused passwords anywhere online, and that protects both their personal and professional accounts.

Safe online behavior is paramount, whether it's at work or in your personal time. Awareness of safe internet practices helps prevent malware infections and data breaches. When something dangerous does set its sights on your network, you will know exactly where to report incidents, and that fast action will help contain and mitigate the impact of a breach much more quickly than a delayed response.

Conclusion

Monthly security awareness training is a vital component of a robust cybersecurity strategy. By keeping employees informed about the latest threats and best practices, you can significantly reduce the risk of incidents.

Security Corner

Are Your Social Media Profiles Secure?

When you join a new social media platform or create a new account, what's the first thing you do?

Hopefully, the answer is: *Turn on specific security settings for your account!*

Why Specialized Security Settings Matter
If you're relying on the default security settings to keep you safe, then you could be at imminent risk of account takeover.

Personalizing your account security protects you from all kinds of cyberattacks!

Why Changing Your Settings Keeps Your Accounts Safe
Seven out of every ten social media users change their privacy settings to manage their online privacy. Are you one of them?

It's never too late to start taking those steps toward better cyber-safety online.

1. **Prevent unauthorized access to your accounts.** Don't share your passwords with anyone!
2. **Protect personally identifiable information** (PII). Proper security settings safeguard your personal information from access or misuse by others.
3. **Enhance your personal privacy**. Adjusting privacy settings allows you to control who can see your posts, photos, and personal details.

Hackers compromise approximately 1.4B social media accounts *every single month*. Make sure to protect yours!

For more information about email-based cyber attacks, call us at 248-362-3800 or visit: https://tinyurl.com/26t4pbtr

Guide To Secure File Storage And Transfers

File storage and transferring hold a very dear place in most people's lives. However, the safety of files is really tough to maintain. In this guide, we are going to help you protect your files. We will explore the various ways to store and send files securely.

What is secure file storage?
Secure file storage protects your files. It prevents others from accessing your files or altering them in any way. Good storage grants lock protection to your files that only you can unlock.

Types of secure storage
Files can be stored securely in various ways, as listed below.
1. Cloud
2. External hard drives
3. Encrypted USB drives

Cloud storage saves files on the internet. External drives save files on a device you can hold. Encrypted drives use special codes to lock files.

Why is secure file storage important?
Secure storage keeps your information private. It stops thieves from stealing your data. It also helps you follow laws about data protection.

Risks of unsecured storage
Unsecured files can lead to huge troubles, including but not limited to:
• Identity theft
• Financial loss
• Privacy breaches

These risks give a reason why secure storage is important. You need to protect your personal and work files.

How Can I Make My File Storage Safer?
You can do so many things to make your storage safer, such as:
• Using strong passwords
• Enabling two-factor authentication
• Encrypting your files
• Keeping your software up to date frequently

Strong passwords are hard to guess. Two-factor authentication adds an extra step to log in. Encryption scrambles your files so others can't read them. Updates fix security problems.

Best practices for passwords
Good passwords are important in keeping your files safer. Here are some tips for creating strong passwords:
• Use long passwords
• Mix letters, numbers, and symbols
• Don't use personal info in passwords
• Use different passwords for each account

What is secure file transfer?
Secure file transfer is a way of sending files safely between individuals or devices. It prevents unauthorized access and prohibits modification of files while in transit. The better methods of transfer protect the files with encryption.

Common secure transfer methods
Here are several ways to securely transfer files:
• Secure FTP (SFTP)
• Virtual Private Networks (VPNs)
• Encrypted email attachments
• Secure file-sharing services

How to Transfer Files Safely?
These steps will keep your files safer while in transit:
• Select a secure method of transfer
• Encrypt the file before you send it
• Give strong passwords for file access
• Authenticate the recipient
• Send the access details separately

How to email attachments safely
• Encrypt important attachments
• Use a secure email service
• Avoid writing sensitive information in the body of an email

Ready to Secure Your Files?
Protect your data from thieves. Use strong passwords, encryption, and safe methods of transfer.

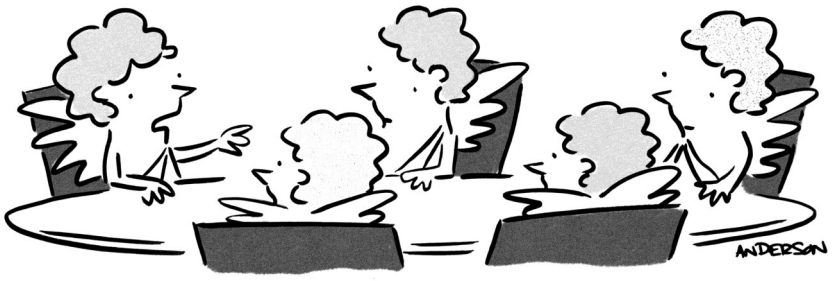
How To Minimize Ransomware Damage

There are many ways to stop ransomware before it hurts you. Here are some key steps:

- **Keep your software up to date**: Always keep your computer and programs up to date. Updates often fix problems that ransomware uses to get in.
- **Use good antivirus software**. Get strong antivirus software. Keep it turned on and updated. It can detect many kinds of ransomware.
- **Be careful with emails**. Don't open emails from people you don't know. Don't click links or download files unless you are sure they're safe.
- **Back up your files**. Copy your most important files and store them on something other than your primary computer. That way, if ransomware locks your files, you'll still have copies.

8 Ways To Organize Your Devices For Productivity

- **Declutter home screen**. Remove unused apps and group similar ones.
- **Organize files and folders**. Set up logical folders and house clean now and then.
- **Organize email**. Create folders and labels. Unsubscribe to unwanted emails.
- **Optimize browser**. Organize your bookmarks and clear your cache regularly.
- **Manage passwords**. Use a password manager.
- **Streamline notifications**. Turn off unnecessary Notifications.
- **Backup data**. Set up automatic backups.
- **Maintain device health**. Update software regularly and run regular scans.



"Last thing, I need everyone to keep March open this year. Word is we're going to be testing out hiding pots of gold to see if we can't pick up some of that market."

9 AI Tools You Need In Your Office For Productivity

AI is going to change how we work. It can make some tasks easier. But it can also cause problems. Let's look at some ways AI can make work tricky.

Where can AI go wrong?

- **Incorrect Information**: It may mix up facts or use data that is too old.
- **Weird outputs**: It may write utter nonsense or create odd images.
- **Biases**: AI can be biased since it learns from data given to it by humans.
- **Job Loss**: Some people fear that AI will steal their jobs.
- **New skills needed**: AI also needs workers to acquire new skills.
- **Teamwork**: The use of AI can affect teamwork between humans.
- **Privacy**: AI requires a lot of data to operate, which causes privacy concerns.

AI can be helpful at work, but it's not perfect. We have to use it with care. If you have questions about using AI at your job, contact us today. We can help you use AI in a smart and safe way.