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

June 2022

Kim Nielsen
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!"

Is Your Security Awareness Training Up To Snuff?

Cybersecurity threats can take many forms and target any individual within an organization. Although high-level security access would be ideal for the hacker, it's effective to crack the passcodes for more accessible employees, who probably have lower levels of cybersecurity threat exposure and training. If they can steal or guess someone's credentials, regardless of whose, they can more easily breach the organization's systems security and steal files off the network.

Since anyone can become a target, it's important for organizations to hold cybersecurity awareness training programs that teaches staff, at ALL levels of the organization, how to recognize and respond to security threats as they arise in real-time. It's not a matter of if a breach happens, its a matter of when a breach happens.

Did you know that 85% of data breaches result from human error?

Whether it's from failing to recognize a threat for what it is or a simple mistake at the end of a long week, one moment of oversight can end up costing the business tens of thousands of dollars to recover from an attack.

One of the challenges in providing thorough cybersecurity awareness training is the changing nature of cyber threats, which advance alongside technology developments. How can you keep on top of the biggest dangers to your business when they are so likely to change?

Supporting Overall Company Security Awareness

Organizations can help their employees grasp the crucial messages of their cybersecurity training by doing some of the following:

- Hold regular training and refreshers to keep everyone appraised of the latest threats

Continued on pg.2

Continued from pg.1

- Find creative ways to bring the point home and keep employees engaged during training
- Include security awareness training in your company onboarding process, to reduce the risk of liability with new hires
- Reward good behavior and, when mistakes occur, educate instead of punish

Go below the surface; while many training programs use a bird's eye view to educate people about common threats, what makes a great training is showing staff how attacks may appear in their particular role and common risk factors involved in that level of the organization. It can be hard to grasp your role in the bigger picture and how a company works *together* to prevent cyber threats.

How to Build Your Internal Training
When creating, expanding or updating your cybersecurity awareness program, what are important aspects to include?

- What to do when someone encounters a threat, including any reporting protocol that must be followed
- How to set up multi-factor authentication on all of their user accounts
- The most up-to-date tactics that cybercriminals use in social engineering attacks
- Education on how and why to update software on a regular basis
- Password security such as using a variety of alphanumerical characters, password managers, changing them routinely and generating different passwords for different accounts
- How to identify safe sites and software
- The dangers of trusting unknown people, wireless networks, and/or devices
- An overview of the threats most likely to target your business, based on its industry or location as well as other factors

> **85% of data breaches result from human error**

Staying apprised of the latest in cybersecurity news will also tell you when there are new technologies or tactics that the company should employ for a more up-to-date security posture.

Conclusion
When it comes to cybersecurity, it takes a village. A strong cybersecurity awareness training program prepares employees for the inevitability of attempted (and successful) breaches, with particular consideration on how their role plays into the greater picture of the company's overall defense posture.

Protect your business from the latest cybercriminal behavior, even as it changes. Regular security training for all levels of the organization will train every employee to keep an eye out for unusual activity on the network, and teach them to avoid those human errors that bad actors take advantage of far too often. Topics like phishing and ransomware are important, but delving deeper into how every individual can take daily steps toward online protection will really make your cybersecurity awareness training successful.

Free Executive Guide: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

PROTECT YOUR NETWORK
"What Every Business Owner Must Know About Protecting and Preserving Their Network"
Don't Trust Your Company's Critical Data And Operations To Just Anyone!

This guide will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at
https://www.cti-mi.com/protectdata622/
or call our office at (248) 362-3800

Security Corner

2 Ways To Tell If A Website Is Secure

These days, it can seem as though the Internet has a scam or trap around every other corner. Whether you're browsing the web in your free time or scouring it for work, many times you'll be clicking on new (and therefore unfamiliar) websites when going about your day. Therefore it's critical to recognize signs that a website is not quite what it seems, and conversely how to tell if the website you're visiting is safe and secure.

HTTP vs HTTPS
Look at the top of any webpage in the URL box. See if it is HTTPS:// instead of HTTP? The "S" stands for *secure*. HTTPS no only transfers your requests, it also encrypts this information for you to seamlessly view the content. It's a semi-complex series of processes that let you view websites in a simplistic and very easy-to-navigate display.

Look For This Symbol
Next to the URL of a secure website, you'll often notice an icon that resembles the outline of a padlock. Hovering your mouse over it, you'll find that it says "Verified by:" or something similar, indicating that it's been adequately vetted and received a digital certificate from a trusted third party company. Companies buy these for their web sites to guarantee that information and communications transmitted over that site cannot be intercepted by outside parties. Data is most vulnerable in transit between secure locations, thus this padlock guarantees your privacy against a man-in-the-middle attack. The creators of fraudulent sites won't bother securing their websites, as it not only creates a trail back to their illegal activity but *costs* money when they're busy trying to *steal* money.

For more information on website security, call us at 248-362-3800 or visit: https://bit.ly/3yHmDBr

Top 5 Cybersecurity Mistakes That Leave Your Data At Risk

The global damage of cybercrime has risen to an average of $11 million USD per minute, which is a cost of $190,000 each second. Of small and mid-sized companies that have a data breach, 60% end up closing their doors within six months of the breach because they can't afford the costs.

The costs of falling victim to a cyberattack can include loss of business, downtime/ productivity losses, reparation costs for customers that have had data stolen, and more. Many of the most damaging breaches are due to common cybersecurity mistakes that companies and their employees make.

Here are some of the most common missteps when it comes to basic IT security best practices.

Not Implementing Muti- Factor Authentication (MFA)
Credential theft has become the top cause of data breaches around the world, according to IBM Security. MFA reduces fraudulent sign-in attempts by a staggering 99.9%.

Ignoring the Use of Shadow IT
Shadow IT is the use of cloud applications by employees for business data that haven't been approved and may not even be known about by a company. Shadow IT use leaves companies at risk for several reasons:

- Data may be used in a non-secure Application
- Data isn't included in company backup strategies
- If the employee leaves, the data could be lost
- The app being used might not meet company compliance requirements

It's important to have cloud use policies in place that spell out, for all employees the applications that can and more importantly, cannot be used for work.

Thinking You're Fine With Only Having An Anti-Virus Application
No matter how small your business is, a simple antivirus application is not enough to keep you protected. In fact, many of today's threats don't use a malicious file at all.
Phishing emails will contain commands sent to legitimate PC systems that aren't flagged as a virus or malware. Phishing also overwhelmingly uses links these days rather than file attachments to send users to malicious sites. Those links won't get caught by simple antivirus solutions. You need to have a multi-layered strategy in place that includes things like:

- Next-gen anti-malware (uses AI and machine learning)
- Next-gen firewall
- Email filtering
- DNS filtering
- Automated application and cloud security policies

Not Having Device Management In Place
A majority of companies around the world have had employees working remotely from home since the pandemic. However, device management policies for those remote employee devices as well as smartphones used for business hasn't always been put in place.

A device management application in place, like Intune in Microsoft 365 can help manage this.

Not Providing Adequate Training to Employees
An astonishing 95% of cybersecurity breaches are caused by human error. Employee IT security awareness training should be done throughout the year, not just annually or during an onboarding process.

Some ways to infuse cybersecurity training into your company culture include:
- Short training videos
- IT security posters
- Webinars
- Team training sessions
- Cybersecurity tips in company newsletters

Phishing Attack Trends

In 2020, 75% of companies around the world experienced a phishing attack.

Phishing remains one of the biggest dangers to your business's health and wellbeing because it's the main delivery method for all types of cyberattacks.

One phishing email can be responsible for a company succumbing to ransomware and having to face costly downtime.

It can also lead a user to unknowingly hand over the credentials to a company email account that the hacker then uses to send targeted attacks to customers.

Phishing takes advantage of human error, and some phishing emails use sophisticated tactics to fool the recipient into divulging information or infecting a network with malware.
Mobile phishing threats skyrocketed by 161% in 2021.

Things You Should Never Do On A Work Computer

Save Your Personal Passwords in the Browser

If your company's network is compromised the malicious actors can leverage your passwords to access your cloud accounts.

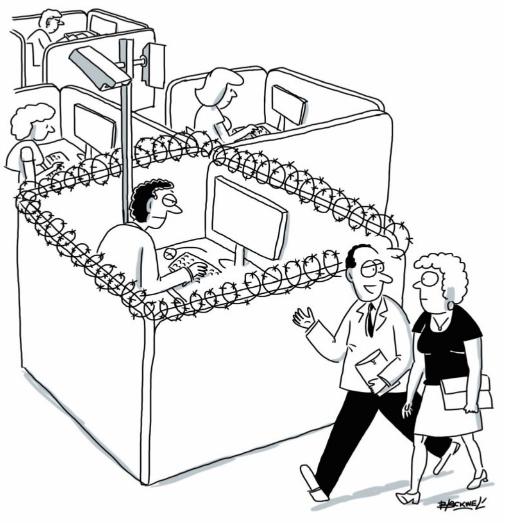
Store Personal Data

This is a bad habit and leaves you wide open to:

- Loss of your files
- Your personal files being company-accessible

Visit Sketchy Websites

You should never visit any website on your work computer that you wouldn't be comfortable visiting with your boss looking over your shoulder.



"HANK'S OUR SECURITY GUY."

CartoonStock.com

Share With Friends or Family

Allowing anyone else to use your work computer could constitute a compliance breach of data protection regulations that your company needs to adhere to.

Google Search Tips

One way you can save time on your personal and work-related searches is to learn some "secret" Google search tips.

These help you narrow down your search results and improve productivity by helping you find the information you need faster.

- **Search a Specific Website Using "site:"** Type in the search bar *site:(site url) (keyword)*

- **Find Flight Information Without Leaving Google** Just type in the flight number and the name of the airlines, for example, type in the search bar *American AA 1977*

- **Look for Document Types Using "filetype:"** Type in the search bar *filetype:(type) (keyword)*

- **Get Rid of Results You Don't Want Using "-(keyword)"** Type in the search bar*(keyword) -(keyword)*

- **Locate Similar Sites Using "related:"** Type in the search bar *related:https://website.com*