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

Hyperlink Safety 101 .....Page 1

FREE Assessment– Is Cloud Computing A Good Fit For Your Company? .....Page 2

Security Corner: What You Need To Know About Physically Securing Your Devices .....Page 3

Should You Spy On Your Team's Daily Work?.....Page 3

Stop Fraud With Your Online Banking .....Page 4

Cool Windows 11 Features You Might Love .....Page 4

March 2023

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!"

Hyperlink Safety 101

Did you know that 20% of the workforce is likely to click on a phishing link? From there, over two-thirds will input their private information into the fraudulent website where they land. That's a HUGE amount of data breaches caused by human error! These can be easily prevented by recalling your Security Awareness Training, but that's not as simple as it seems.

When threat actors are devising their plan of attack, they often study their target organization or individual first, so as to deliver more plausible falsehoods and entrap more victims. For example, a hacker might do preliminary surveillance to find out when you do bank deposits and where, so that they can more realistically pose as your service provider and coerce money transfers or financial accounts from you. Once they've crafted a viable ruse, they often send out false messages pressuring you to act fast and click on a provided hyperlink to solve the purported issue.

STOP RIGHT THERE!

Before you click on it, you need to assess if it is from a *reliable source* or part of a *criminal scheme* to steal your private data.

The Truth About Suspicious Links

It can be difficult to tell whether certain messaging are a scam or not. While some spam is easily identifiable by its rampant spelling errors and outright lies, other hackers will go to great lengths to disguise themselves as your boss asking for account verification, or a service asking you to secure an existing account. In 2021, phishing messages were most likely to

Continued on pg.2

Continued from pg.1

contain subject lines like…

- Odd activity on your account
- Remote Working Satisfaction Survey
- Upcoming Changes (usually to your account or our policies, etc.)
- Your access has been temporarily disabled…

The goal is to convince you to click the link they provide in the message to solve the problem as quickly as possible – when really the threat actor has already set up a fake website landing page to capture your login credentials. They try to engender panic, anger, excitement or some other pressing emotion so that you act without thinking too hard about the risks.

Unmasking the Danger

Even if you feel compelled to act on the message, or you aren't sure if it's legitimate (even real accounts can be hacked, after all!), there are a few ways to check what's on the other end of a hyperlink WITHOUT clicking on it. Some websites deliver **drive-by malware** just by landing on the homepage, so you don't want to proceed before finding out where it leads.

1. Hyperlinks can look like anything; you can have a link that says Covergirl.com but it really leads to Google
2. If you hover your mouse over a link, but don't click, then a popup should appear after a moment showing the full URL
3. Alternatively, you can right-click links to copy the source URL and then paste it into a new tab, without hitting the search button or past it into Word to review it first.
4. Check to see where it's really redirecting you before you search!

This will DRASTICALLY reduce the number of hackers who breach the network or steal personally identifiable information (PII). Other signs that you're looking at a phishing message include minor inconsistencies in the domain of the sender (i.e. appie.com instead of apple.com); they don't address you by name or mention any specifics; and unfamiliar people CC'd on the email.

Conclusion

This is why your annual Security Awareness Training is so important, and so is keeping up with the latest threats to your job position! Cybercriminals are always looking for new ways to deceive you into handing over your information, or even just dropping your guard low and long enough to mistakenly allow them access to confidential data. It's important, not only to pay attention during your Awareness Training, but subsequently to refresh your knowledge of cybersecurity defense tactics so you remain prepared whether your official Training and Compliance Assessments took place last week or eleven months ago!

Take control of your cyber-safety, and the security of all the private information on your home and work networks, by being careful where you click. When human error accounts for 95% of data breaches, added caution and investigation really does protect your systems from hackers.

Free Assessment: Is Cloud Computing A Good Fit For Your Company?

While there are a ton of benefits to cloud computing, it's NOT right for every company. Some applications don't play well in the cloud. You need commercial-grade Internet connectivity, and some functions, like working with big graphics files, are better kept local or the slowness will make you crazy. However, in almost every case, parts of your computer network (functions) can easily be put in the cloud to save you money and give you better service. So before you get rid of your server and sign up for a service like Microsoft 365, it's important you talk to someone who can honestly assess your unique situation and tell you the pros and cons of making the switch to cloud computing.

We are offing a FREE Cloud Readiness Assessment to any business or government organization with 10 or more PCs and a server. At no cost or obligation, we'll come to your location and conduct a complete review of your computer network, data, software, hardware and how you work. From there, we'll provide you with insights and helpful answers as to how you could benefit from cloud computing.

Claim Your FREE Assessment Today At:
https://www.cti-mi.com/cloudassessment323/

Security Corner

What You Need To Know About Physically Securing Your Devices

A lot of cybersecurity awareness revolves around the digital security of all your devices…but how well do you take care of their *physical* security? Thieves can steal your laptop out of your bag. Then, they can crack your password and steal all your data directly!

3 Tips for Better Physical Security

1. Lock up important devices when you're not using them, whether that's leaving your cubicle to use the bathroom for a few minutes or keeping your home office locked when you throw a party.

2. Leave it home if you're not going to use it. Although we can't all stand to have our cell phones away from our person for that long, maybe you can re-think bringing your laptop on vacation or while going to the coffee shop.

3. Keep your eyes on ONLY the files you're supposed to have access to. **You are responsible for abiding your clearance level.** You are just as capable of committing insider threats as anyone else in the organization — even by accident!

Conclusion
The physical security of your devices is just as important as their cybersecurity. Understanding some of the ways that threat actors compromise devices by their direct hand, facilitates understanding some simple ways to protect your tech on a daily basis.

For more information about SPAM and other cyber threats, call us at 248-362-3800 or visit: https://bit.ly/3wGBA4y

Should You Spy On Your Team's Daily Work?

Since the pandemic, employers around the world have needed to change. They've had to shift how their employees operate. Remote work is very much here to stay. Organizations and employees can both benefit from the work-from home and hybrid work revolution.

Cost savings is a driver for supporting remote work. Employee morale and productivity also can be higher when employers grant this flexibility.

A majority of organizations support some type of remote work. Statistics show that:
• 16% of companies are completely remote
• 40% support hybrid office/remote working
• 44% don't allow employees to work remotely

While there are benefits, there are also challenges to this new environment. Employers worry about the cybersecurity risks of remote teams. Managers can find it more challenging to make sure employees are doing what they should do.

The remote and hybrid work environment has led to the rise of employee monitoring tools. These tools have received mixed reviews from employees.

WHAT IS EMPLOYEE MONITORING SOFTWARE?

Employee monitoring software tracks digital movements. This can include everything from general clock-in clock-out tracking to taking screenshots of an employee's computer several times per hour.

Tracking tools like Hubstaff and BambooHR track many activities on a person's computer. The information is then sent in a daily or weekly report to the company. Items that these tools can track are:
• Time clock
• Keyboard activity
• Keystrokes
• Mouse activity
• Websites visited
• Screenshots of the desktop
• Apps used and how long in use

The most invasive of tools can even track the sounds and video of the employee.

Tracking can be visible, so the employee knows about it, or the tracking can be completely hidden from the employee.

It depends on the tool used and the cultural and ethical considerations of the employer. This type of monitoring can benefit an organization worried about "productivity theft." But it can also alienate good employees and torpedo morale and trust.

Let's go through the pros and cons before you set up this type of system.

MONITORING TOOLS PROS

1. Understand Time Inputs
Knowing exactly how much time employees spend on a project can help with future ROI projections.
2. Reduce Time Wasting
About half of monitored employees spend 3+ hours per day on non-work activities. When employees know that their boss is monitoring their app usage, they're less likely to goof off.
3. Billing Time Tracking
If you invoice your clients based on time, Monitoring Tools can help capture the teams time correctly so it's billed properly. This stops hours falling through the cracks.

MONITORING TOOL CONS

1. Hurts Team Morale
Many employees feel they are put in a cage when monitoring is introduced. Morale can plummet, which takes productivity and trust along with it.
2. Activity isn't Productivity
Many tools simply report on keyboard and mouse activity. But what if the employee must solve a workflow issue and needs to use their brain for a few hours, not their mouse?
3. Good Employees Leave
Nearly half (47%) of surveyed tech employees said they would quit if their boss tracked them.

Stop Fraud With Your Online Banking

Millions of dollars are stolen from small business bank accounts around the world every single month (and the threat is increasing every single day).

As hackers get smarter and build new ways to break into your systems, you need to work hard to stay one step ahead of them so you don't fall victim.

Here are some essentials you need to have in place with your Online Banking:

- Have a Strong & Unique Banking Password
- Turn On Two-Factor Authentication
- Set Up Banking Alerts

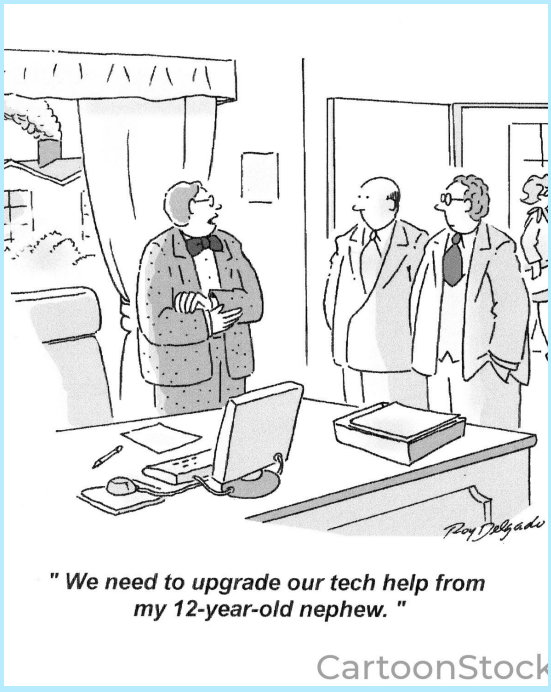
Cool Windows 11 Features You Might Love

Every time Microsoft releases a new Operating System, some people love it and some people hate it. (although I think we can all agree that *everyone* hated Windows Vista).

Here are some areas in Microsoft's Windows 11, that Microsoft has focused on to help you work easier and faster:

- Snap Layouts
- Master Search
- Clipchamp Video Editor
- MS Teams Video, Audio & Text Messaging

You'll also notice they have redesigned and centered the Start Menu /Task Bar, perhaps taking inspiration from Apple's Mac.



5 Ways To Prevent One Of The Most Common Sources Of Data Breaches

Misconfiguration of Cloud Solutions is often overlooked when companies plan Cybersecurity Strategies. Cloud apps are typically quick and easy to sign up for so users often assume that they don't need to worry about Security because it's handled.

This is a bad assumption because Cloud Security is a shared model. The Provider/ Vendor handles securing the backend infrastructure. But the user/client is responsible for configuring security settings in their account.

Here are some tips to help improve Cloud Security:

- Enable Visibility Into Your Cloud Infrastructure
- Restrict Privileged Accounts
- Put in Place Automated Security Policies
- Run Regular Security Setting Audits
- Ensure each user has their own Account