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

August 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!"

How Much Does Your Smart Phone Know?

The Internet of Things, commonly known as IoT, refers to handheld devices like phones and tablets that you use to get online whenever you're away from your computer. Even television come as a Smart TV now; IoT is everywhere. Look around you and count how many IoT devices you can see right now.

With increased IoT usage comes the proliferation of viruses and threats that basic computer firewalls can prevent, but which devices like your smart phone often aren't equipped to combat. Who, then, can access your cellphone, and exactly what can they find when they do?

The Android Malware
People joke all the time that their Internet browsers are listening in on their conversations, given how targeted ads have become. For some Android users, that became frighteningly real when news broke of the malware called Process Manager.

Not only does it record everything you say, but can track your location, see pictures, read call logs, and view and even send texts. The icon for the malicious app looks like a gear so victims think that it's a legitimate Android program. In the background, though, it's secretly downloading an app from the Google Play Store; the threat actors profit every time a new user downloads the app.

When the app starts running, the icon disappears – but Android users can still recognize the malware as a notification in the pulldown menu. Now that you think about it, has your phone been malfunctioning lately?

Continued on pg.2

Continued from pg.1

Amazon Alexa Gone Wrong

Devices like the Google Home, Amazon Echo, Apple HomeKit, and Samsung SmartThings are pitched as voice-activated helpers around the home, but they've been the subject of multiple hacks over the years including a recent vulnerability being dubbed **Alexa vs. Alexa**.

The attack occurs when a threat actor gets close enough to connect a Bluetooth device to third- or fourth-generation Amazon Echos. By pairing the device to their own nearby, a hacker can give voice commands and get the Alexa to effectively "hack" itself, by issuing the command aloud and then following it as if given by a real person. Alexa is programmed to follow any command given that it's preceded by the correct "wake word," which is either Alexa or Echo, provided the command is stated at the right volume as well.

This hack is dangerous because smart devices like these are often connected to other smart appliances, can make phone calls and purchases from the victim's account, acquire PII and account information, affect finances, mess with your calendar, and even unlock smart doors.

Brightest Bulb in the Box

Unlike the others, Sengled designed their smart lightbulbs to delve into the user's life. These lights connect to Bluetooth and monitor a person's health. Aside from tracking sleep, body temperature and heart rate – yes, seriously – it can even tell if somebody has fallen down. It's set to release in late 2022.

The announcement of this product came with news of the company's new TV light strips, which use a remote camera to sync colored lights to whatever is occurring on the screen.

Although these products haven't launched yet, they effectively demonstrate just how far along smart technology has come. If hackers can track your phone's location via Android malware, what will they do with a Wifi-connected camera in your living room and light that logs your every move?

Conclusion

The Internet of Things has its uses, both the good and the bad. As in all aspects of the tech industry, hackers adapt almost as fast as we learn how to stop them. What's important is recognizing the depths of what information can be mined off of your cellphone or the daily habits processed through a smart home device. Then you can make more informed decisions about your online safety and just how much time you really spend connected to the world wide web – even when you don't think of it as accessing the Internet in a traditional, monitor-and-keyboard sense.

Smart devices, like the phone in your pocket, can keep track of your location, texts, calls, photos and so much more personal data. Be careful about what you reveal online so your IoT network keeps working for you, and you alone.

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/cloudassessment722/

Security Corner

Don't Download That File! And Other Things To Know About Email Security

Email revolutionized the way that we communicate with each other. Even as people moved more toward personal devices to communicate with friends, email remains a critical part of many people's lives – particularly in the business world. Cybercriminals know this, and target victims accordingly. What cyber-threats should you be aware of so that you can continue emailing safely and securely?

Phishing
By purchasing a list of emails and associated names, hackers can send **phishing scams** to an amassed list all at once, and even address recipients by first name so the message seems more personal and believable.

BEC Scams
Business email compromise (BEC) scams, appear to be from your organization or connected to it professionally in some way. Usually the scam messages will come from an address very similar to one you know and trust, but with an extra letter or punctuation.

Suspicious Attachments
Always be wary of email attachments, especially if you don't recognize the sender. Even messages that seem real can be fraudulent. Cybercriminals know how important email is for most people, just as much as you do. Keep it a safe haven for work and connection by practicing cybersecurity every time you log on.

For more information about email security, call us at 248-362-3800 or visit: https://bit.ly/3uHGk9v

How Often Do You Need To Train Employees On Cybersecurity Awareness?

You've just completed your annual phishing training where you teach employees how to spot phishing emails. You're feeling good about it, until about 5-6 months later when your company suffers a costly ransomware infection because someone clicked on a phishing link.

You wonder why you seem to need to train on the same information every year, and yet still suffer from security incidents. The problem actually is that you're not training your employees often enough.

People can't change behaviors if training isn't reinforced regularly. They also tend to easily forget what they've learned after several months go by.

So, how often is often enough to improve your team's cybersecurity awareness and cyber hygiene? It turns out that training every four months is the "sweet spot" when it comes to seeing consistent results in your IT security.

Why Is Cybersecurity Awareness Training Every 4-Months Recommended?
There was a study presented at the USENIX SOUPS security conference that looked at users' ability to detect phishing emails versus how often they were trained on phishing awareness and IT security.

Employees were tested at several different time increments:

- 4-months
- 6-months
- 8-months
- 10-months
- 12-months

It was found that four months after their training, they were still able to accurately identify and avoid clicking on phishing emails. However, after 6-months, their scores started to get worse. Then they continued to decline further the more months that passed after their initial training.

So, to keep employees well prepared to act as a positive agents in your overall cybersecurity strategy, it's important they get training and refreshers regularly.

Tips on What & How to Train Employees to Develop a Cybersecure Culture
The gold standard for employee security awareness training is to develop a cybersecure culture. This is one where everyone is cognizant of the need to protect sensitive data, avoid phishing scams, and keep passwords secured.

Unfortunately, this is not the case in most organizations. According to the 2021 Sophos Threat Report, one of the biggest threats to network security is a lack of good security knowledge and practices.

The report states, "*A lack of attention to one or more aspects of basic security hygiene has been found to be at the root cause of many of the most damaging attacks we've investigated.*"

Well-trained employees significantly reduce a company's risk of falling victim to any number of different online attacks. To be well-trained doesn't mean you have to conduct a long day of cybersecurity training every four months. It's better to mix up the delivery methods.

Here are some examples of engaging ways to train employees on cybersecurity that you can include in your training plan:

- Self-service videos that get emailed once per month
- Team-based roundtable discussions
- Security "Tip of the Week" in company newsletters or messaging channels
- Simulated phishing tests
- Cybersecurity posters
- Celebrate Cybersecurity Awareness Month in October

Get More Unplugged Laptop Time With These Battery –Saving Hacks

Laptops today boast ridiculously powerful batteries, a far-cry from the roughly 2-3 hours we used to get. Most Apple laptops nowadays can easily provide up to 12 hours of battery life.

So, if you're laptop battery doesn't seem to get you past a few hours of use, try the following tips:

- Lower the Display Brightness
- Reduce PC Battery Use in Power/Sleep Settings
- Enable Battery-Saver Mode
- Use the Manufacturer's Battery Calibration Tool
- Use Microsoft Edge Browser on a PC or Safari on an Apple for their Efficiency Settings
- Turn Off Unnecessary Apps
- Don't Expose Your Laptop To Extreme Temperatures

Home Security: Why You Should Put IoT Devices On A Guest Network

The number of internet connected devices in homes has been growing exponentially over the last decade. A typical home now has more than 10 devices connected to the internet.

IoT stands for Internet of Things, and it basically means any other type of "smart device" that connects online besides computers and mobile devices.

Here are two alarming statistics that illustrate the issue with IoT security:

- During the first six months of 2021, the number of IoT cyberattacks was up by 135% over the prior year.
- Over 25% of all cyberattacks against businesses involve IoT devices

Hackers Use IoT Devices to Get to Computers & Smartphones

Smart devices are a risk to any other device on a network because they are typically easier to breach, so hackers will use them as a gateway into more sensitive devices, like a work computer.

Improve Security by Putting IoT on a Separate Wi-Fi Network

Just about all modern routers will have the ability to set up a second Wi- Fi network, called a "guest network."

By putting all your IoT devices on a separate guest network from your devices that hold sensitive information, you eliminate that bridge that hackers use to go from an IoT device to another device on the same network.
Just make sure that you secure your Guest Network with a strong passphrase.

Need Help Upgrading Your Home Cybersecurity?

With so many remote workers, hackers have begun targeting home networks because they can target your sensitive data in a typically less secure environment than they would face in a business setting. Work with an IT profession to help get this setup correctly.

"Is that computer, down there, the one you were having problems with?"