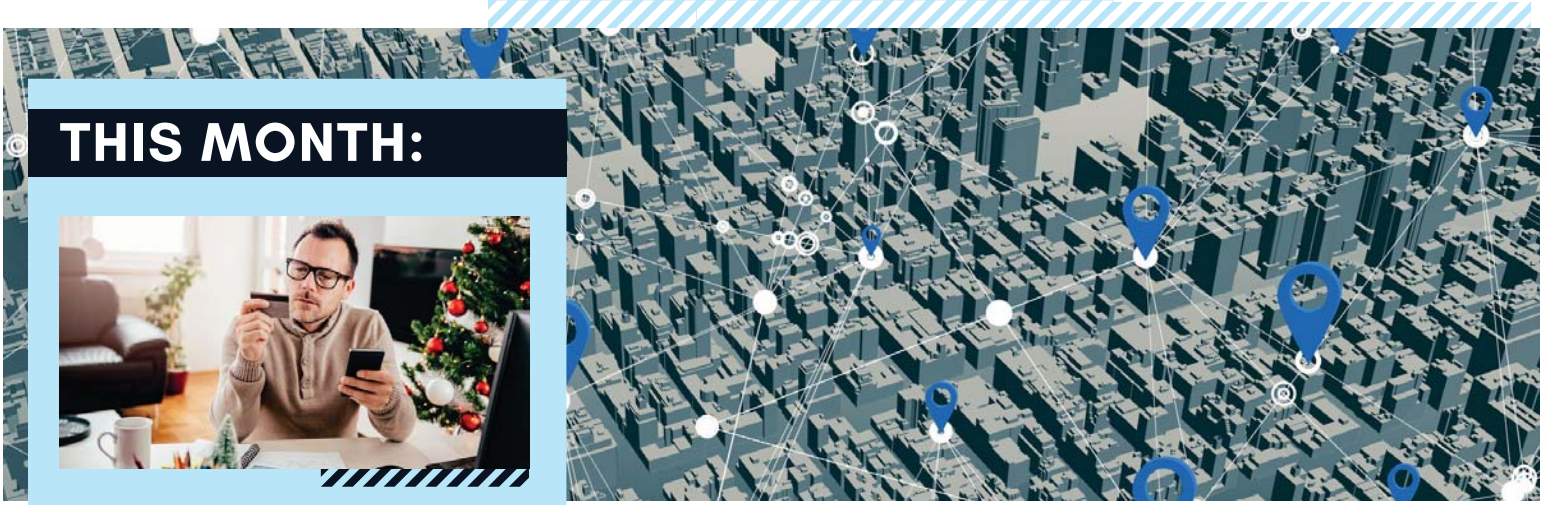
CYBER TIMES

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



THIS MONTH:

One of the world's most popular travel seasons is quickly approaching: the winter holidays. Despite the radio hits chiming something about being "the most wonderful time of the year," expenses, travel and an increase in scams are enough to raise the blood pressure of even the jolliest among us. Don't rush to the spiked eggnog just yet – we've got some tips to make this season as cheery and bright as it should be.

This monthly publication is provided courtesy of Rick Rusch, CEO of Secure ERP, Inc.

OUR MISSION:

Too many businesses are exposed and vulnerable to cyber attacks. With a unique Guardian Angel Protection solution, our clients get back to their business and sleep better knowing their data is secure.

HERE'S WHAT GOOGLE MAPS TIMELINE KNOWS ABOUT YOU (AND IT'S MORE THAN YOU THINK)

It's 10 p.m. – do you know where your children are? Google probably does. Thanks to Google Maps' Timeline feature, the tech company probably knows where your whole family has been – down to the GPS coordinates. The feature was first rolled out in 2015 on Android devices and two years later on Apple, but many people still don't know how much information the app actually collects. Before you hit the road this holiday season, take a minute to review your privacy settings to see if the risk is worth the benefits.

What Google Maps Timeline Can See

With Google Maps Timeline, you can go back to any day and see in detail where you were, when and for how long. For example, the map will show you when you left work, got home and any pit stops you made. It can also tell if you traveled by bike, car, train or bus. If you haven't changed the settings, this information may have been stored for YEARS. This kind of tracking is helpful if you forget the name of a lunch place you visited last month with an amazing chicken wrap. However, if you care about your privacy and prefer not to have your home address or daily jogging routine under Google's watchful eye, you need to turn this feature OFF.

Pros And Cons

Under the guise of being a digital assistant, Google collects that information to make your life easier. At the same time, it's creating detailed profiles of all of us. In some ways, this makes our lives easier. In other ways, it invites severe risks.

Upsides

- Find what's lost: Has your kid ever lost their phone during an errand spree and is not sure if they left it in the cart at Target or the bathroom at The Cheesecake Factory? Yeah, it's not a good feeling. If your phone is connected to the Internet, Google Maps Timeline can retrace your steps.

continued on page 2...

...continued from cover

- Peace of mind: Many parents gain peace of mind about their children's safety by knowing where they are and where they've been.
- In business: Employers can also use the feature to ensure employees working remotely are where they are supposed to be when they are supposed to be there.
- Tailored ads: Because Google apps speak to each other, your ads and recommendations are customized to your lifestyle.

Downsides

- Peeping Toms: Anyone who gets hold of your account can build a profile of you. They know where you live, work and hang out. Threat actors weaponize profiles in extortion schemes or impersonate people to commit other heinous crimes.
- Not 100% accurate: You must be connected to the Internet and logged in to Google for the feature to work.

> **Before you hit the road this holiday season, take a minute to review your privacy settings to see if the risk is worth the benefits.**

- A lot less privacy: It's creepy when an app tracks and stores personal information!

How To Turn Tracking OFF

If you don't feel like having Google's eyes on your every move, follow these steps on one of your devices to update the settings. Here's how to do it from your computer:

Change Settings Using Your Computer:

1. Log in to your Google account.
2. Tap your profile icon or initials, and select "Manage Your Google Account."
3. Click on "Data & Privacy."
4. Scroll to "History Settings" and select "Location History."
5. Pause your history.
6. BONUS TIP: Delete your timeline history by going to Maps Timeline, "Manage Location History," and selecting an auto-delete option.

Tips For Using Google Maps Timeline

If the benefits outweigh the risks for you or your family, do two things. First, define a timeline to delete stored data. You can delete your location history after 3, 18 or 36 months – or keep it forever (which we don't recommend). Once you pick an option to remove the data, Google is legally obligated to delete it.

Second, use multifactor authentication on your devices and accounts so that even if someone finds your phone or hacks your account, they can't get in. Take control of your privacy and review this buried feature in Google's Maps app!

FREE REPORT DOWNLOAD:

If You Are Considering Cloud Computing For Your Company, DON'T, Until You Read This...

If you are considering cloud computing or Office 365 to save money and simplify IT, it is extremely important that you get and read this special report: **"5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud."**

This report discusses in simple, nontechnical terms the pros and cons of cloud computing, data security, how to choose a cloud provider and three little-known facts that most IT consultants don't know or won't tell you about cloud computing that could end up causing you MORE problems and costing you more money than you anticipated. **Even if you aren't ready to move to the cloud yet**, this report will give you the right information and questions to ask when the time comes.

Get Your FREE Copy Today:
www.secureerpinc.com/cloudreport

CARTOON OF THE MONTH

"A hacker logged into my fitness tracker and stole all my steps!"

WFH STRATEGIES THAT *ACTUALLY* WORK

We all value work and family balance. But during the holidays, that seesaw tends to teeter more toward family, even when end-of-year deadlines hang over our heads. No one wants to be the office jerk who says NO to flexible work schedules. However, if you say yes, you may open your business up to lowered productivity and increased security risks – unless you have clear WFH strategies.

A recent study by Tenable found that 67% of business-impacting cyber-attacks targeted remote employees. Working remotely is like having your cake and eating it, too. Still, it's entirely appropriate to ask your employees (and yourself) to not eat the cake off the floor or in bed. What we mean is that to support your employees' productivity and company security, make sure you're implementing some Work From Anywhere (WFA) best practices. Just as they should eat their cake at the table, if your employees are going to work from home or Grandma's basement, they need to check that their setup meets simple expectations.

WFH/A Best Practices:

Have A Decent Internet Connection.
Most video calls require at least 5 Mbps, but 50–100 Mbps ensures multiple people can stream at once without issues.

Access Shared Company Resources.
Make sure employees have tested their connection off your company's network BEFORE they leave. Can they access the VPN? Are their login credentials stored safely in a password manager?

Have A Place To Work.
Preferably a room with a door (that closes … and locks). Nobody wants Grandma crashing a Teams meeting. Noise-canceling headphones are also an excellent idea.

Agree On Core Working Hours.
If your employees are working remotely (not taking vacation), make sure they've agreed to be available at certain times, including team meetings. Yes, this means they can't watch their kids and should have child care set up.

Have A Project.
Especially for short-term WFH situations, having a clearly outlined deliverable is an easily tracked productivity metric. They either got it done or they didn't.

Have A Cyber Security Policy.
According to Tenable's survey, 98% of remote workers use a personal device for work every single day. A cyber security policy includes all aspects of your company, not just remote work. However, remote work is unique, and you may need to take extra steps to protect your business if remote work is happening at your company. This includes installing security software on devices and enforcing multifactor authentication on their device, on work applications and when accessing the company's network. Train your team on at-home security, like how to spot phishing e-mails, create strong passwords and keep kids or other family members away from work devices.

Remember …

Nobody wants to get tied up in a security snafu or lose productivity over remote work. Make remote work policies a core pillar of your company so that whenever an employee requests to work remotely, you have a policy in place to ensure they can do their best work and do it safely!

Christmas Gift Suggestions:

To your enemy, forgiveness.
To an opponent, tolerance.
To a friend, your heart.
To a customer, service.
To all, charity.
To every child, a good example.
To yourself, respect.

– Oren Arnold,
novelist, journalist and humorist

3 Million Mail Servers AT RISK

There's a problem with Exim, a mail transfer agent that is used by more than 3 million mail servers globally.
Exim has significant vulnerabilities (notably CVE-2023-42115, CVE-2023-42116, and CVE-2023-42117), which means that if you use Exim your system could be exposed to unauthorized remote code execution. This could allow malicious code that is complex and difficult to detect to be put into your system.

Let us help. Our expertise lies in shielding businesses from such vulnerabilities. You can ensure your organization's communication remains uncompromised by taking the simple step of reaching out to us for a quick cyber security assessment. We can also address potential remediation approaches.

We're here to safeguard your systems against emerging threats.

Guardian Angel Protection by Secure ERP, Inc.

AIRLINE TICKET SCAMS ARE SOARING

INSIDE THIS ISSUE

CISCO AT RISK

A critical security flaw has been found in Cisco devices running IOS XE software. The flaw lets attackers secretly create super admin accounts on those devices. Millions of devices worldwide run that software. Tens of thousands have already been compromised.

Immediately, do the following:

1. Updating all devices to the latest version of IOS XE.
2. Checking device logs for unusual activity or files.
3. Disabling devices' HTTP Server function wherever it is not absolutely necessary.

We've addressed this problem for our clients. We just want to ensure you are aware of the situation.

Scammers love travel season. They know your eyes are peeled for a cheap ticket and have devised convincing ways to get their hands on your money. Tricked consumers have spent months of their lives dealing with the consequences of these scams and lost thousands of dollars in the process. In a recent plague of travel scams, criminals are pretending to be "travel agents" selling plane tickets. Between 2020 and 2021, digital fraud in travel and leisure increased 68.4% globally, according to TransUnion's 2022 Global Digital Fraud Trends Report.

How Plane Ticket Scams Work

Travel scammers use a handful of tactics to steal your information. They create fake websites, pose as travel agents and send you "confirmation" e-mails that don't include an airline ticket. Some call your phone to "confirm your information" for a flight, asking for your credit card, bank or personal information. Or they use social media ads or e-mails advertising free or cheap tickets. These are all major red flags to watch out for. Before clicking or booking anything, pay attention to these travel tips to avoid getting scammed out of thousands of dollars of your hard-earned vacation savings.

Here's How To Avoid Travel Scams

1. *Always verify that an agent or agency is legit.* In the U.S. and Canada, you can use the Better Business Bureau (BBB) or travel associations like the International Air Transport Association to verify agent credentials. Read customer reviews and look for weird grammar errors in e-mails and on websites. However, the BBB recommends booking directly through hotels or airlines.

2. *Check for a ticket confirmation number.* If you don't get a ticket number with your confirmation e-mail, a scammer may have reserved you a seat instead and stolen your money.

3. *Watch out for online deals.* Scammers use fake e-mails and ads to boast amazing deals on hotels or flights. If you think they are too good to be true, they are.

4. *Be skeptical of "confirmation calls."* If you get a follow-up call from an agent to verify your personal information, it's probably a scam.

Stay informed, pay attention and implement these practical tips for your next adventure. Safe travels!