CSU Connection December 2023

You take care of running your business, we'll take care of your technology.

Should Your Business Follow Google's Security Lead?

Google has introduced a new security strategy – but **is it right for *your* business?**

It has put some employees on a cyber diet, restricting their internet access to limit potential threats.

On the surface, it sounds like a smart move. Google's approach is like building a taller fence around your house to keep out burglars.

By reducing internet connectivity, they're effectively shrinking their digital footprint and making it harder for cyber criminals to find a way in.

But is it foolproof?

Well, **not exactly.**

While this strategy does limit external threats, it doesn't entirely eliminate the risk.

Think of it this way: you've built a towering wall around your house, but your teenager leaves the back gate open. Similarly, internal systems might remain connected to other devices that can access the internet, providing a potential entry point for cyber threats..

In other words, you can't just focus on keeping things out.

Yes, there are very real threats from external hackers using all sorts of techniques like phishing, zero-day attacks, and malware. But the security industry often overlooks significant threats from within the perimeter.

Research shows that insider threats account for 62% of all security breaches.

These insiders – disgruntled employees, careless staff, or malicious actors – often have legitimate access rights, intimate knowledge of the system, and can bypass traditional security checks. It's like having a burglar who knows where you hide your spare key.

So, what's the takeaway?

While Google's strategy has its merits, it's not a one-size-fits-all solution. Just as you wouldn't wear shoes that are too big, your business needs a cyber security strategy tailored to fit its unique requirements. A robust cyber security strategy should focus on both external and internal threats and have measures in place to mitigate risks from all angles.

Our advice? Instead of simply following in Google's footsteps, consider your own business's needs and vulnerabilities. And of course, if you need help with that, get in touch.

Gadget of the Month:

Titanium Micro Mercury

Introducing the **Titanium Micro Mercury External SSD** – a pocket-sized powerhouse! Crafted from *spaceship-grade titanium*, it's tough, compact, and up to *5x faster* than conventional portable HDDs.

Additionally, it features a built-in tracker for added security. The Titanium Micro Mercury External SSD is not merely a storage device, but **a sophisticated solution** for all your data needs.

Get yours at: https://www.titaniummicro.com

Most Secure Way to Share Passwords with Employees

Breached or stolen passwords are the bane of any organization's cybersecurity. Passwords cause over 80% of data breaches. Hackers get in using stolen, weak, or reused (and easily breached) passwords.

But passwords are a part of life.

Since you can't get around passwords, how do you share them with employees safely?

One solution that has gained popularity in recent years is using password managers.

Why Use a Business Password Management App?

Here are some of the reasons to consider getting a password manager for better data security.

- **Centralized Password Management**

A primary advantage of password managers is their ability to centralize password management. They keep employees from using weak, repetitive passwords. And from storing them in vulnerable places.

- **End-to-End Encryption**

Leading password managers use robust encryption techniques to protect sensitive data.

- **Secure Password Sharing Features**

Password managers often come with secure password-sharing features. They allow administrators to share passwords with team members. And to do this without revealing the actual password.

- **Password Generation and Complexity**

Password managers typically come with built-in password generators. They create strong, complex passwords that are difficult to crack.

- **Secure Sharing with Third Parties**

Password managers offer secure methods for sharing credentials with third-party collaborators or contractors.

Smart Home Tech You Should Adopt and Avoid

In the age of smart living, our homes are becoming increasingly intelligent. They're designed to cater to our every need. Smart gadgets are transforming how we turn on the lights, home security, and more. They even help us feed our pets from afar.

But with the rapid evolution of this technology, it's crucial to make informed choices.
To know what to adopt and what to avoid. Every smart technology isn't as helpful as another.

Here are some tips on what smart home tech to adopt and to avoid:

Adopt: Smart Lighting Systems

Smart lighting systems have proven to be both energy-efficient and convenient. They allow you to control the ambiance of your home. As well as schedule lights to go on and off. You can even change colors to match your mood.

Avoid: Cheap, Unbranded Smart Devices

There is a definite allure to lowcost smart devices. Yet these unbranded alternatives often compromise on security, support, and functionality. This is true for both security and performance.

Investing in reputable brands ensures several benefits. Including:

-Regular updates
Security patches
-Compatibility with other smart home devices
-Long-term support

Adopt: Smart Thermostats

Smart thermostats learn your habits. They adjust your home's temperature accordingly. They contribute significantly to energy savings. They do this by optimizing heating and cooling based on occupancy patterns.

Avoid: Overcomplicating Security Systems

Robust security systems are essential. But overcomplicating them with unnecessary gadgets may lead to confusion and inefficiency. The more devices you add to a security system, the more exposure for your network.

Adopt: Smart Home Hubs

Smart home hubs are popular. They give you one place to manage all your smart devices and enable seamless communication between them. Investing in a compatible hub ensures a harmonious smart home experience.

Avoid: Ignoring Privacy Concerns

The convenience of smart home tech should not come at the expense of your privacy. Be cautious about devices that constantly record audio or video. Especially if done without clear user consent. Reg larly review privacy settings. Limit data collection. Choose devices from reputable companies that focus on user privacy and data security.

Adopt: Smart Home Security Cameras

Smart security cameras provide real-time monitoring and remote access. They also enhance the safety of your home. Look for cameras with features like motion detection, two-way audio, and cloud storage.

Avoid: Impulse Buying Without Research

The excitement of new gadgets can lead to impulse purchases. Before buying any smart home device, conduct thorough research. Read reviews and compare features.

Sing Along With Us to This [Remastered] Holiday Classic!

It's the Most Vulnerable Time of the Year (Hackers Version)

It's the most vulnerable time
of the year
With passwords a-leaking
And systems a-creaking,
hackers drawing near!
It's the most vulnerable time
of the year!

It's the hap-hackiest
season of all...
With malware e-greetings,
and crooks all competing,
to exploit it all!
It's the hap-hackiest
season of all

There'll be tree
trimming parties
Throwing back hot totties
Family gathered around,
There'll be cookies a baking
And mall trips partaking
Distractions will only compound

It's the most vulnerable time
of the year
With phishing emails
Dressed like holiday tales,
click on one and Oh Dear!
It's the most vulnerable time
of the year!

There'll be tree
trimming parties
Throwing back hot totties
Family gathered around,
There'll be cookies a baking
And mall trips partaking
Distractions will only compound

It's the most vulnerable time
of the year
There'll be much hacker action
But give them no traction,
we want to be clear!

It's the most vulnerable time
It's the most vulnerable time

It's the most
vulnerable time
of the year!

12 Online Holiday Security Risks that Only a Grinch Could Love!

1. Fake Shipping Notifications
Do NOT click on ANY tracking links from FEDEX, UPS, or the USPS. Instead, go directly to their website and type in the tracking number in question or log in to your account and check open orders directly.

2. Email Deals
If a sale sounds too good to be true, it probably is! Ask yourself, "Did I sign up for emails from this retailer? If you're really interested in the sale, go to the retailer's website or check with customer service to see if the sale is real.

3. Bogus Charities
The holidays bring out the best in us and the worst in the bad guys! Most legitimate charity websites use .org, not .com. Also, beware of charities with copycat names or small variations in the spelling of the website. The best policy is to visit their website directly instead of clicking on email links.

4. Gift Cards
Got an email from your boss telling you to purchase gift cards? STOP – don't do it! Verify the request with a phone call. Most banks and insurance companies are refusing to refund money stolen this way.

5. IRS & Other Government Emails (Scams)
During the holiday's, aggressive criminals pose as IRS agents with the intention of stealing money or personal information. The IRS will never call you to demand payment, they always communicate via a letter first and then a certified letter.

6. Online Shopping
To avoid ransomware and other "nasties" it's best to type in the URL of your favorite shopping sites. If you must click when shop-surfing, only click top-ranked search results.

7. Long-lost Friends Scams
It's easy to spoof someone's email address if you have their contact list. If you haven't talked to someone in a long time or if the email sounds "off" the best policy is to pick up the phone and ask if they sent you the email. Whatever you do, do NOT reply to the email!

8. Santa Letter Scams
Cybercriminals manipulate parents' heartstrings by offering great deals on "Santa letters." Always check reviews, the BBB, and Consumer Affairs before using one of these services. *Do NOT provide personal details like birthday, school, or pet name about your kids/grandkids.

9. Social Media Ads
Criminals can easily replicate a legitimate ad (Best Buy, Amazon, Macy's), and when you click on it, spyware can be installed on your phone or other devices. During the holidays, refrain from clicking on ads on your phone. It's harder to tell it's a scam, and it's easier for the bad guys to steal your information.

10. Pet Scams
Pet scams are often difficult to avoid as cute pictures and good deals pull at the heartstrings and wallet. Only purchase pets through reputable sources such as Petsmart, the local shelter, breeders that can provide references, or other local adoption agencies to prevent this fraud.

11. Emailed Holiday & eGift Cards
These cards are popular and easy to send. Here are some clues that can help you spot a fake e-card: spelling mistakes and poor grammar, cards asking for personal account information (Home Depot, Lowes, Amazon, etc.) to "verify" your identity. Never install .exe files.

12. Travel Deals
We all want an all-inclusive trip to London or the Caribbean for $299 – but let's face it, those deals are either a scam or a timeshare sales pitch! If it sounds too good to be true, it probably is!

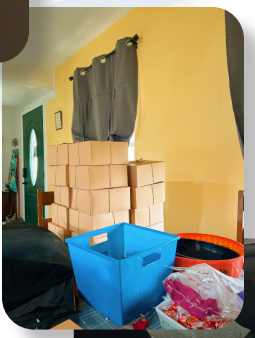
What's Up With The CSU Team?

Alyssa supports "Hockey Fights Cancer" night with the Washington Capitals!

Welcome our newest addition to the CSU family: Cheems!

She loves to oversee all our daily work!

Workin' hard and sending thank-filled gifts to our clients!



We love it when former employees come to visit!

Faye was so happy to see her best friend Dave.

Drum roll please... Help us welcome CSU's newest employees!

Welcome our new client care dispatcher, Paola!

Paola's favorite NFL team is the Pittsburgh Steelers, and she loves comedy movies. Her favorite actor (like Chuck) is Adam Sandler!

Paola

Welcome our new technician, Byron!

Byron's favorite breakfast food is a steak, egg, and cheese bagel. Yum!

His favorite movie is currently "Captain America: Civil War"

Byron

Welcome another technician, Johnny!

One of Johnny's hidden talents is playing the cello!

His favorite movie is Baby Driver!

Johnny

Stay connected with us!

Instagram:
computer_services_unlimited

Facebook:
Computer Services Unlimited Inc.

Phone:
(703) 968-2600

Digital Version of Newsletter:
www.csuinc.com/news

Our Services:

- -Data Backup & Recovery
- -Managed Services
- -IT Consulting
- -Network Security
- -Cloud Computing
- -Remote IT Services
- -Cyber Security Training
- -Mobile Device Management

We believe that experienced, reputable and fast responding IT support should be the standard.

CSU COMPUTER SERVICES UNLIMITED

Our mission is to deliver outstanding IT support to your business in order to improve uptime, productivity, and profitability.

COMPUTER SERVICES UNLIMITED

CSU Connection

December 2023

You take care of running your business, we'll take care of your technology.

in this issue...