THE CYBERSIDE BRIEF

Insider Wisdom from 20 Years of IT Defense for Your Business Prosperity and Security

INSIDE THIS ISSUE

This monthly publication is provided courtesy of Patrick Birt, President of AdRem Systems Corporation.

HACKERS ARE WATCHING:

Follow These Simple Steps For Safe Holiday Traveling

As holiday travel picks up, hackers see a prime opportunity to exploit travelers who may let their guard down on their digital security. Security risks like phishing, public WiFi and lost devices can easily compromise your personal information during travel. But it's not just your data at stake – when employees let their guard down, they can unknowingly open the door to threats for their entire company.

According to World Travel Protection, only about 30% of companies require employees to follow basic cyber security measures while traveling. This leaves a significant gap in protection, potentially exposing entire organizations to serious risks. Here's how to safeguard yourself and your business during busy holiday travel.

Safety Tips For Before, During And After A Trip

To avoid the stress of lost devices, stolen data or a security breach that could ruin your trip, make cyber security a priority by taking a few simple steps before, during and after your journey.

BEFORE YOUR TRIP

1. Update All Devices

Software updates often include patches for security vulnerabilities.

2. Back Up Important Data

If your laptop containing vital client presentations is stolen, a cloud-based or other secure backup will allow you to get your data back without significant disruption.

continued on page 2...

...continued from cover

3. Use Multifactor Authentication (MFA)

MFA adds an extra layer of security by requiring more than just a password to access accounts. This makes it much harder for hackers to gain access, even if they have your password.

4. Restrict Access To Sensitive Data

If you don't need certain files or applications while on the road, temporarily remove access. This reduces the risk of compromised sensitive information if your device is stolen or hacked.

5. Secure Your Devices

Ensure all devices are password-protected and encrypted. Encryption scrambles your data, making it unreadable to unauthorized users.

SAFE PRACTICES WHILE TRAVELING

1. Avoid Public WiFi

If you must connect, use a virtual private network (VPN) to encrypt your Internet traffic. This acts as a secure tunnel between your device and the Internet, protecting your data from prying eyes.

2. Be Cautious Of Public Charging Stations

Public USB charging stations can be compromised by attackers looking to steal data or install malware on your device – a practice known as "juice jacking." Plug your charger into an electrical outlet or use a USB data blocker, which prevents data transfer.

3. Never Leave Devices Unattended

Always keep your devices with you or securely locked away. If you must leave your laptop in your hotel room, use a physical lock to store it. Never hand your device to strangers, even if they appear to be offering help.

4. Disable Bluetooth

Turn off Bluetooth when not using it, especially in public places. Hackers can exploit open Bluetooth connections to gain access to your devices.

5. Pay Attention To Online Activity

Phishing, business e-mail compromise and online shopping scams are common during the holiday season. Always verify the authenticity of e-mails, especially those requesting sensitive information or urgent action.

RETURNING HOME: POST-TRAVEL SECURITY CHECK

Security awareness doesn't stop once you get home. Sometimes, you don't know until you return that you've been hacked.

1. Review Account Activity

Once you're back home, review your accounts and look for unusual logins or transactions you didn't initiate.

2. Change Passwords

If you accessed sensitive information while traveling, it's a good idea to change your passwords when you get home. This ensures that any potential compromises during your trip don't lead to long-term issues.

Consider A Company-Wide Travel Policy

To further protect your business, consider implementing a company-wide travel cyber security policy. This policy should outline the expectations and procedures for employees traveling on business or working remotely. Key elements to include are:

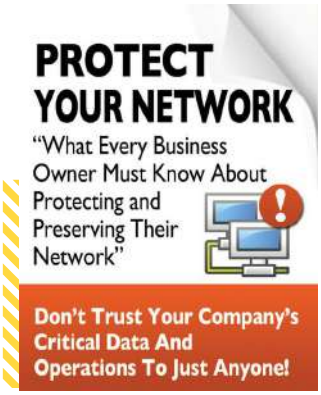
- Guidelines for using public networks
- Reporting lost or stolen devices
- Responding to potential security incidents

Following these simple steps will significantly reduce travel-related cyber security risks and ensure that you can travel with peace of mind.

FREE REPORT:

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

This report 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 www.AdRem.com/protect or call our office at (703) 860-2233.

SAFE CYBER PUZZLE

SECURE OUR WORLD

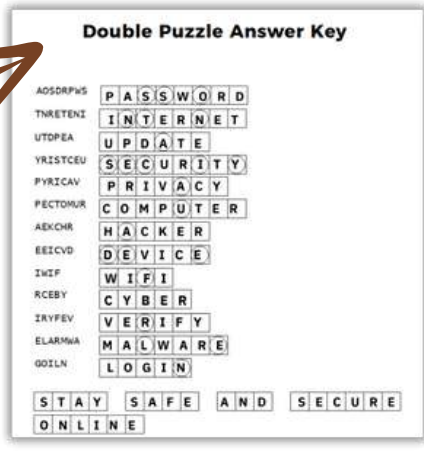
Find the Cyber Terms!

Update
Cookies
Encrypt
Email
Internet
Password
Phish
Malware
Data
Hacker
Virus
Ransomware
Login
Firewall

E	V	W	X	U	P	D	A	T	E	L	O	R	P
I	N	T	E	R	N	E	T	D	F	O	V	I	S
N	B	H	A	C	K	E	R	T	I	G	V	X	R
O	E	R	J	M	X	E	K	B	R	I	W	W	A
V	O	T	E	C	Y	F	J	X	E	N	N	K	N
I	O	U	W	A	F	Y	K	I	W	G	D	D	S
R	L	P	V	O	C	P	B	Y	A	E	D	A	O
U	U	O	A	R	R	H	V	K	L	N	A	N	M
S	W	R	G	S	E	K	J	Q	L	C	T	A	W
M	T	T	U	S	S	M	W	H	K	R	A	H	A
D	V	S	J	E	O	W	A	W	J	Y	T	D	R
C	O	O	K	I	E	S	O	I	F	P	E	T	E
E	G	U	P	H	I	S	H	R	L	T	J	K	Z
T	M	A	L	W	A	R	E	A	D	T	P	S	U

October Answer Keys

Safe Cyber Puzzle



Trivia

Answer C:

Despite its name, it's actually made of a copper-nickel "shielding" fabric and claims to deflect WiFi and 5G electromagnetic waves.

Look for answers in Next Month's issue or download at: https://www.adrem.com/puzzle/

GIVE THE GIFT OF YOUR UNDIVIDED ATTENTION WITH NOTIFICATION GROUPING

Constant notifications can be a relentless distraction, pulling you out of meaningful conversations. This holiday season, group your notifications to collapse multiple notifications and instead receive a summary and turn off topics you actually don't want to see. Then devote that free time to your family and friends as you celebrate!

In your iPhone, go to Settings -> Notification and choose the app you want to get notifications from. Next, tap Notification Grouping. Then you can pick from Automatic, By App or Off. To group notifications, choose By App. For Android users: Go to Apps & Notifications in Settings. Tap to see the list of all your apps and pick the ones you want to group notifications for. Next, tap Notifications. Then, look for an option called Notification Grouping or Bundled Notifications and turn this feature on or customize it based on how you want app notifications grouped. Voilà!

CARTOON OF THE MONTH

Take the groundhog - now *that's* a sweet gig."

Compliancy Navigator

The Cost of Non-Compliance

A CASE FOR PROACTIVE COMPLIANCE MANAGEMENT

Non-compliance isn't just a minor oversight – it's a business risk with real financial, reputational, and operational impacts. Whether a business is navigating HIPAA for healthcare data, aligning with NIST standards for federal work, or working toward CMMC certification for DoD contracts, meeting compliance requirements has become essential. However, many organizations underestimate the cost of non-compliance until they face an audit, fine, or breach. Let's look at why proactive compliance management isn't just beneficial – it's critical.

RISKS OF NON-COMPLIANCE

When an organization fails to meet compliance standards, the repercussions move beyond fines. Penalties for HIPAA violations, for example, can reach up to $1.5 million per violation, depending on severity. CMMC compliance, meanwhile, is a requirement for retaining certain federal contracts, with non-compliance potentially meaning the loss of lucrative opportunities. Beyond direct costs, compliance violations can also damage an organization's reputation. In industries that handle sensitive data, such as healthcare or defense contracting, clients demand trust. A single breach or penalty can lead clients to take their business elsewhere, causing a loss of revenue and long-term credibility.

OPERATIONAL DISRUPTION

Addressing non-compliance after a violation often means urgent, disruptive changes to workflows, systems and training. Many organizations find themselves scrambling to implement compliance measures urgently, which diverts resources from other projects. A proactive approach to compliance, on the other hand, allows for a phased, manageable integration of compliance standards into daily operations, minimizing disruptions.

WHY PROACTIVE COMPLIANCE MANAGEMENT MATTERS

Proactive compliance management means treating compliance not as a checklist but as a continuous process integrated into the organization's strategy and culture. By assessing risks, educating staff, and regularly auditing compliance measures, businesses can stay ahead of regulations, protect their reputation, and secure their financial future. Taking a proactive approach not only keeps your organization compliant but also allows you to leverage compliance as a competitive advantage.

If you're ready to strengthen your compliance posture, Sherpa is here to help – call or visit us online.

PRESENTED TO YOU BY SHERPA, AN ADREM SYSTEMS COMPANY:

SHERPA An AdRem Company SYSTEMS

theSherpa.us | 571-360-3926 | info@thesherpa.co

Celebrating Team Achievements

After a failed attempt to sell to Blockbuster, Netflix founder Marc Randolph made a life-altering decision: if you can't join 'em, beat 'em. Despite being $50 million in debt, Netflix ultimately succeeded in toppling the video rental giant within a decade. While this story is often seen as a beacon of hope for start-ups, it teaches established companies a different lesson: the real threat may come from an unexpected competitor who targets your weaknesses, not your strengths. Randolph says, "If you're not willing to disrupt yourself, you're leaving it wide-open for someone to disrupt your business for you."

Having worked with numerous early-stage companies, Randolph has identified five key elements that foster innovation and help companies disrupt their markets – or defend against those disruptions. These ideas provide a road map for thinking like a start-up, no matter the size of your company.

1. Innovation Can Happen Anywhere

You don't need to be in Silicon Valley to innovate. Randolph notes, "I just got back from Australia, where I saw a company using drones to implant seeds for reforestation by firing them into the ground from 60 feet up." The Internet has leveled the playing field, making it possible for anyone, anywhere, to develop groundbreaking ideas.

2. You Don't Need To Be A Genius Or Have Special Skills

Randolph knows entrepreneurs from all walks of life. One dropped out of college and transitioned from driving an ambulance to fighting forest fires before starting his own company. Another, a musician who spent a decade in a ska band, created and sold a music-streaming service. Even teenagers are making waves in the business world. "I've found that the most disruptive people are not the A or B students," Randolph says. "They're the C students who managed to navigate the education system without having all the risk-taking squeezed out of them."

3. Embrace Risk, But Not Recklessness

A successful innovator embraces calculated risks that come from starting down a path without knowing exactly where it leads. "If you wait until you've figured out what's around the corner through analysis and research, someone's already beaten you there," Randolph advises.

4. Generate Ideas – Lots of Them

To innovate, you need more than just one good idea – you need hundreds. "It doesn't matter if they're big ideas or even particularly original ones," Randolph says. The Post-it Note, for example, which sells nearly a billion dollars' worth every year, wasn't groundbreaking but proved immensely successful. Knowing in advance if an idea is good or bad is impossible. The only way to find out is to take that risk, build something and put it to the test.

5. Confidence Is Key

Finally, you need confidence in your ideas, even when life gets in the way or others doubt you. "Everyone who has ever taken a shower has had an idea," Randolph quotes Nolan Bushnell, founder of Atari. "But it's the person who gets out of the shower, towels off and does something about it who makes the difference."

OUR SERVICES

IT BUSINESS SOLUTIONS

Managed and Co-Managed Service (MSP)
Managed Security Service (MSSP)
Cloud Computing
VoIP Solutions
Data Backup and Recovery
Cybersecurity
Vendor Management
Hardware as a Service (HaaS)
Secure Access Service Edge (SASE)
Virtualization
Remote Work Environments

COMPLIANCE SOLUTIONS

CMMC, NIST, HIPAA, ISO, FTC, etc.
Email Enclaves
Employee Security Training
Data Backup and Recovery
Data Privacy and Encryption
Disaster Recovery Planning
Penetration Testing
Vulnerability Scanning
Policy Consulting
Cybersecurity Consulting

HARDWARE PROCUREMENT

Shop.AdRem.com

HOSTING & ONLINE SERVICES

OnlineServices.AdRem.com

Domain Registration and Transfer
Website Hosting: Website Builder & WordPress
Website Security Solutions
Custom Website Design
WordPress Website Support Solutions
Logo Design
Virtual Private Servers (VPS)
Dedicated Servers
Email Marketing

AdRem SYSTEMS

OUR MISSION

To apply our 20 Year Legacy of knowledge and innovation, to defend Critical IT Networks, and encourage a more secure nation of Tomorrow by delivering Today's technologies with respected, trusted, and proven individuals.

UNREASONABLE HOSPITALITY

By Will Guidara

Will Guidara was only 26 when he took over the run-down brasserie Eleven Madison Park and transformed it into a Michelin three-star-winning, world-class restaurant within 11 years. His secret sauce? Over-the-top, out-of-the-box and exceptional hospitality that customers couldn't forget. *Unreasonable Hospitality* by Will Guidara offers valuable insights for business leaders who don't want to provide simple customer service but rather an extraordinary customer experience. His innovative strategies, like creating bespoke guest experiences and fostering a culture of thoughtful communication within his team, provide practical takeaways for any industry. This book encourages leaders to rethink how they engage with customers and employees, illustrating that extraordinary service can turn routine interactions into powerful, memorable experiences that drive long-term success.

TECH GIFTS TO AVOID BUYING

While a playful robot that uses facial recognition to analyze a child's moods might seem like an awesome gift for your nephew, it's not so great when you learn that data can be hacked by cybercriminals or shared for third-party advertising.

At the 2023 CES electronics exhibition, Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency, told the Washington Post that most tech companies address safety problems when they happen rather than developing safety features proactively. Companies are "really focused on cost, capability, performance and speed to market, not on basic safety," she said.

No matter how well they promise to clean your floors or entertain your children, some tech products are not worth the security risks. Here are a few tech gifts to avoid and tips for wiser tech shopping.

Beware These Tech Gifts

Camera-Enabled Devices With Bad Privacy Policies

Doorbell cams have one purpose: to see and hear everything around your home and neighborhood. Then it sends that data to the cloud. Poorly secured cameras could allow hackers to access live feeds, potentially giving them insight into when you're home and when you're away. Always choose devices with end-to-end encryption and transparent privacy policies.

AI-Integrated Devices

In 2022, images from iRobot's AI-enabled Roomba were leaked online. Although the company claimed test users consented to share data, it underscores the risk of AI devices collecting extensive information about you. Read the privacy policy closely. If you can't customize data settings or companies aren't clear about how they use your data, shop elsewhere.

Tracking Devices For Kids

Tracking devices for children might seem like a thoughtful gift for families, but these devices can expose children's real-time location to hackers, stalkers or third parties. In 2021, the popular family safety app Life360 was found to be selling user location data to data brokers, according to reporting by The Markup. A safer approach is to discuss location sharing openly with your kids and use built-in features like Google's Family Link or Apple's end-to-end encrypted location sharing.

Genetic Testing Kits

In 2023, nearly 7 million 23andMe users had their ancestry data hacked – a stark reminder of the risks of genetic testing. Criminals are drawn to this highly sensitive data, and companies like Veritas and Ancestry.com have also faced breaches. Beyond theft, there's the issue of law enforcement's ability to access this information. Remember, once you spit into a test tube, you give away your genetic information, that of your close relatives and even future generations.