



## 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 Wi-Fi 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 cybersecurity 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.

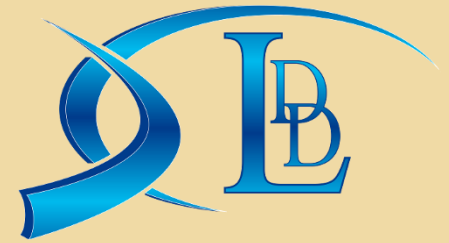
#### Safety Tips: Before, During and After a Trip

To avoid the stress of lost devices, stolen data or a security breach that could ruin your trip, make cybersecurity 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.
- 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

*Continued on pg.2*



November 2024



This monthly publication provided courtesy of David Luft, CEO of LDD Consulting, Inc.

#### Our Mission:

*We promise to provide knowledgeable, courteous and prompt service. We care as much about your business as you do. If you are not completely satisfied, be sure to let us know. If we cannot resolve the issue, we will refund your money.*

... continued from cover

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 Wi-Fi:** 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 cybersecurity 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 cybersecurity risks and ensure that you can travel with peace of mind.

**FREE DOWNLOAD:**

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

Considering cloud computing or Office 365 to save money and simplify IT? Then, you need this report: *“5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud.”* Discover the pros and cons, data security issues, choosing a provider, and three crucial facts most IT consultants overlook. Get informed to avoid unexpected costs and issues, whether you're ready to move to the cloud now or later.



**Get your FREE copy today: [www.LDDconsulting.com/cloud-free-report](http://www.LDDconsulting.com/cloud-free-report)**

**3 REASONS TO BE THANKFUL**  
For Tech

- Enhanced Security
- Reliable Performance
- Efficient Recovery



# Marc Randolph Explains How to Get Your Company Thinking Like a Start-Up



After a failed attempt to sell to Blockbuster, Netflix founder Marc Randolph made a pivotal decision: if you can't join them, beat them. Despite being \$50 million in debt, Netflix eventually succeeded in toppling the video rental giant within a decade. This story, often seen as a beacon for start-ups, offers established companies a crucial lesson: the real threat may come from unexpected competitors targeting your weaknesses. Randolph states, "If you're not willing to disrupt yourself, you're leaving it wide-open for someone to disrupt your business for you." Drawing from his experience with early-stage companies, Randolph has identified five key elements that foster innovation and help businesses disrupt their markets or defend against disruptions. These ideas serve as a roadmap for thinking like a start-up, regardless of your company's size.

## 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."

## Client Spotlight

### LDD Gives Us Convenience, Efficiency & Productivity

Having LDD as our IT provider gives us total peace of mind. I only communicate with one entity for all our tech needs, saving time. LDD techs remote in and fix issues quickly and efficiently, which is a huge relief. With LDD, I don't worry about IT hassles or maintenance—I can focus on my clients, our #1 priority.



*Michelle Diamond-Reece  
President  
Mark Diamond's Jewelers  
Albuquerque*



### 1 Give the Gift of Your Undivided Attention with Notification Grouping

Constant notifications can distract you from meaningful conversations. This holiday season, consider grouping your notifications to receive summaries and turn off topics you don't want to see. This way, you can devote more time to family and friends while celebrating!

For iPhone users, go to Settings -> Notifications, select the app, and tap Notification Grouping. Choose Automatic, By App, or Off, then select By App to group notifications.

For Android users, navigate to Apps & Notifications in Settings, select the apps you want to manage, and tap Notifications. Look for an option called Notification Grouping or Bundled Notifications and enable it or customize your preferences. By organizing your notifications, you can enjoy a more focused and meaningful holiday!



**Making Technology Work for You**  
 2420 Midtown PL NE, Suite K  
 Albuquerque, NM 87107

PRST STD  
 US POSTAGE  
 PAID  
 ABQ, NM  
 PERMIT 1187

Return Service  
 Requested

## Inside This Issue

Hackers Love Holidays — Make Sure Your Family and Your Employees are Protected this Season | 1

It's Not the Idea, It's the Action: Netflix Founder's Blueprint for Business Success | 3

«Name»  
 «Company Name»  
 «Street Address 1» «Street Address 2»  
 «City», «State» «Postal Code»



## TECH GIFTS TO AVOID BUYING

A playful robot using facial recognition to analyze a child's moods might seem like a great gift, but it poses risks when data can be hacked or shared for advertising.

At the 2023 CES, Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency, said most tech companies address safety issues reactively. They prioritize cost, capability, and speed to market over safety.

No matter how well they clean or entertain, some tech products carry security risks. Here are a few tech gifts to avoid and tips for smarter 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.