NEWSLETTER

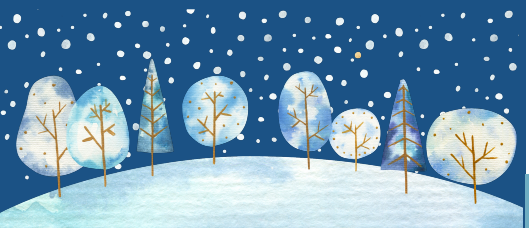
RJ2 Technologies Monthly Newsletter
December 2024

1701 Golf Road
Suite T3-300
Rolling Meadows, IL 60008

(847) 303-1194

www.rj2t.com

In this newsletter:



Happy Holidays from RJ2 Technologies!

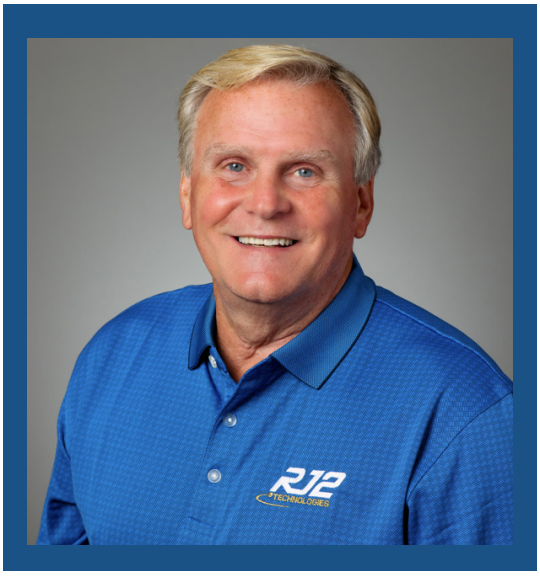
Dear valued clients, partners, & team members,

As we approach the end of another remarkable year, I would like to take a moment to express my gratitude to each of you for your unwavering support and dedication.

This holiday season is a time for celebration and reflection. I encourage you to take this opportunity to recharge, spend quality time with loved ones, and celebrate the sucesses we have achieved throughout the year.

Thank you again for your support and dedication. Wishing you all a joyous holiday season and a prosperous new year.

Warm regards,



Jeffery Dann

President of RJ2 Technologies

This Year's Biggest Data Breaches

According to TechCrunch, this year has seen some of the most damaging data breaches in history. In 2024 alone, hackers stole billions of personal records, and it's possible your data is among those stolen records. Let's look at this year's record-breaking attacks and what you need to know about protecting your information.

1. National Public Data (2 Billion-Plus Records)

What happened: In December 2023, hackers accessed the systems of National Public Data, a background-check company. In April, 2.7 billion records with highly sensitive data for 170 million people were leaked onto the dark web.

Who is exposed: The stolen data includes records for people in the US, Canada and the UK.
Compromised data: 2 billion-plus records containing full names, current and past addresses, Social Security numbers, dates of birth and phone numbers.

2. Change Healthcare: (38 Million Records)

What happened: In February, the UnitedHealth-owned tech firm Change Healthcare was compromised by a Russian ransomware gang that gained access through systems unprotected by multifactor authentication. The attack caused widespread downtime for health care institutions across the US and compromised data for many, many Americans. UnitedHealth paid $22 million to prevent data leaks, but another hacker group claimed to still have some of the stolen Change Healthcare data.

Who is exposed: Estimated data exposure for one-third of the American population (likely more).
Compromised data: Payment information, Social Security numbers and medical data, including test results, diagnoses and images.

3. AT&T (Compromised TWICE)

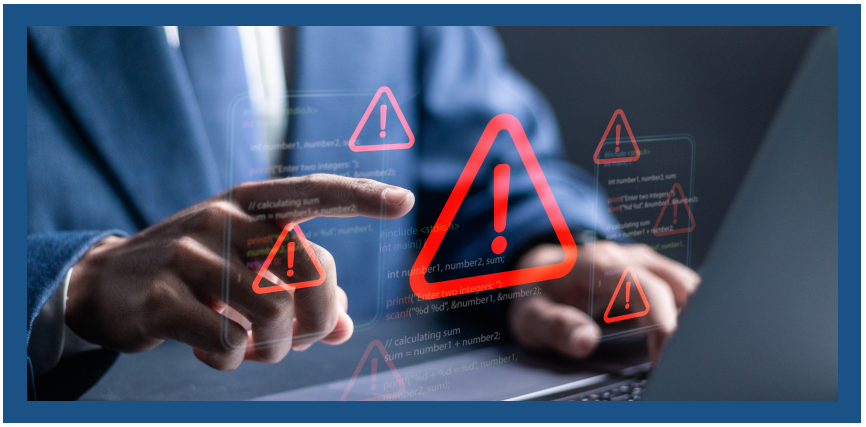
What happened: In March, hackers released data for more than 73 million past and existing AT&T customers going back to 2019. Then, in July, data was stolen from an AT&T account the company had with data giant Snowflake (more on that below). Reportedly, AT&T paid a ransom to the hackers to delete the data. However, if this data is leaked, it could expose the data of anyone called by AT&T customers, including noncustomers.

Who is exposed: 110 million-plus past and current customers and, potentially, noncustomers.
Compromised data: Personal information, including Social Security numbers and phone numbers.

4. Synnovis (300 Million Patient Interactions)

What happened: In June, a UK pathology lab, Synnovis, was attacked by a Russian ransomware gang. The attack resulted in widespread outages in health institutions across London. Reportedly, Synnovis refused to pay the $50 million ransom.

Who is exposed: Past and existing patients in the UK.
Compromised data: 300 million patient interactions, including blood test results for HIV and cancer, going back many years.



5. Snowflake (600 Million-Plus Records And Growing)

What happened: In May, cloud data giant Snowflake announced a system breach caused by stolen employee credentials. Hundreds of millions of customer records were stolen from Snowflake customers, including 560 million from Ticketmaster, 79 million from Advance Auto Parts and 30 million from TEG.

Who is exposed: Millions of customers from many of Snowflake's 165 corporate customers, including those mentioned above, plus Neiman Marcus, Santander Bank, Los Angeles Unified School District and many more.
Compromised data: Customer records.

How To Protect Yourself Personally

In this day in age, everyone should protect themselves. However, you can prevent the situation from being worse for YOU by taking a few extra steps to protect your data. Here's what to do:

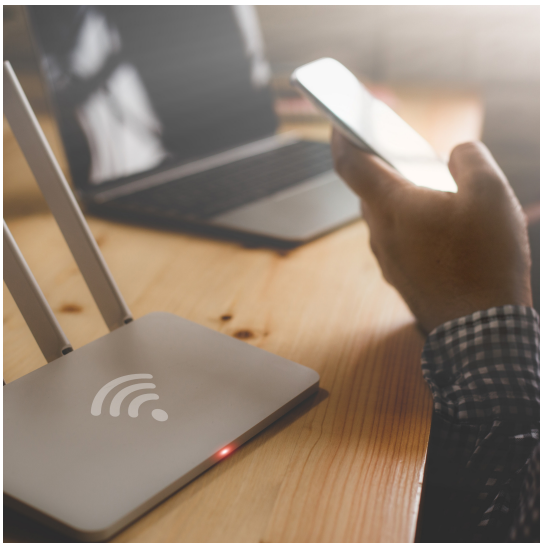
- Review your health-related communications: With so many breaches affecting health institutions this year, pay attention to your statement of benefits and look for services you didn't receive. If you spot something suspicious, notify your health care provider and insurance company right away.
- Freeze your credit: This will stop anyone from opening a credit card or loan in your name.
- Update your log-in credentials: If any account was compromised, change all passwords to all log-in accounts like your bank, credit card, or medical. Set up alerts too, so you're immediately aware of any unusual activity. A password management system can help manage this effectively.
- Be wary of e-mails: After a breach, hackers access all kinds of information and may use that to send fraudulent e-mails. Slow down, read carefully and verify requests before taking any action.

Vendor Partner Highlight

VONAHI SECURITY

Vonahi Security is a cybersecurity SaaS company that automates network penetration testing. Vonahi strives to resolve current and upcoming cybersecurity challenges for all business sizes, including MSPs and internal IT teams. Their innovative automated penetration testing platform, vPenTest, provides continuous, real-time assessments of cybersecurity risks. vPenTest helps identify vulnerabilities, perform exploits, and enhance security postures efficiently.

With this partnership, RJ2 Technologies can ensure our clients receive top-tier, automated security testing that keeps their networks safe and secure. To learn more about this partnership, **call RJ2 Technologies at 847-303-1194 or email marketing@rj2t.com.**



Beware of WiFi Squatting

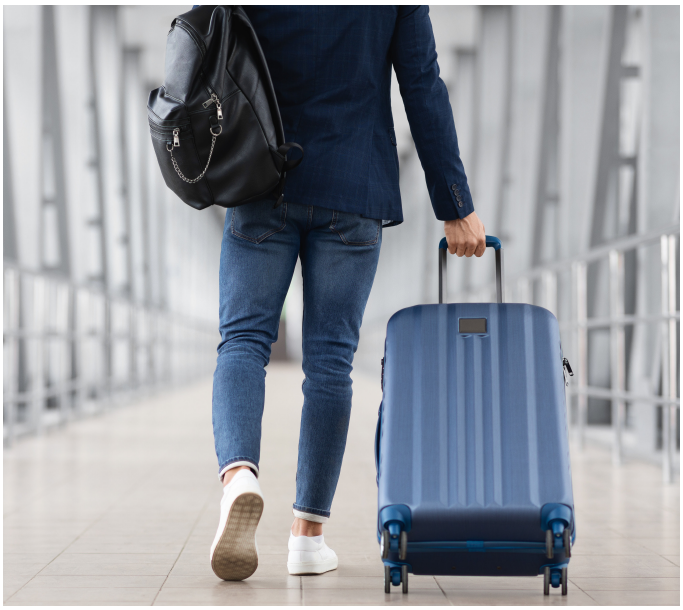
When did you last check who has access to your WiFi network? If it's been a while, you'll probably be surprised by who's hanging around. Managing your WiFi access is an important step to keeping your data safe because unwanted WiFi squatters could, at best, slow your WiFi speeds and, at worst, have access to any device or file connected to your network, like household security cameras.

To see who has access to your WiFi, find your router's IP address (you can find instructions online about how to do this), type the IP address into your browser and log in. Next, look for a list called "DHCP Client" or "Connected Devices." Review the list, and if any unknown devices are on it, update your WiFi password and reconnect only the devices you trust.

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.



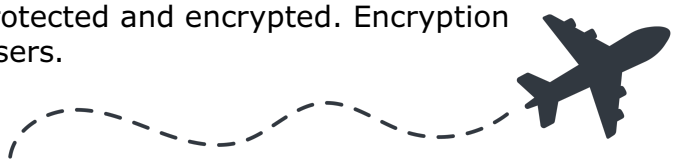
Safety Tips for Before, During and After a Trip

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.

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 compromised.
5. Secure Your Devices: Ensure all devices are password-protected and encrypted. Encryption scrambles your data, making it unreadable to unauthorized users.



Safety 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 compromised.

1. Review Account Activity: Once you're back home, review your bank 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. For more information on safe traveling practices, please **call RJ2 Technologies at 847-303-1194 or email marketing@rj2t.com.**

Enjoying Getting the Most Recent IT News from RJ2 Technologies?

Follow us on our social media pages for more IT content, latest tech trends, company updates, tech tips and more. Connect with the RJ2T family and show your support!

@RJ2Technologies @RJ2Technologies @RJ2Technologies

@RJ2Technologies @RJ2Technologies532

Vendor Partner Highlight

Nodeware is a vulnerability management platform that provides non-disruptive scanning of assets. They provide vulnerability data with actionable remediation. This AI-driven solution provides internal and external scanning. We are happy to be in partnership with Nodeware to ensure our customers have have continuous protection against cyber threats. that is non-disruptive and have real-time protection capabilities. This partnership allows us to enhance our cybersecurity measures, ensuring our clients benefit from robust, continuous protection against potential threats. To learn more, please **call RJ2 Technologies at 847-303-1194 or email marketing@rj2t.com.**