NEWSLETTER

RJ2 Technologies Monthly Newsletter
September 2024

1701 Golf Road
Suite T3-300
Rolling Meadows, IL 6000

(847) 303 -1194

www.rj2t.com

In this newsletter:

What Do You Do When a Company Compromises Your Data

With the rise in cyber-attacks worldwide, you've likely received more than one notification from a company you work with informing you that your data has been compromised in a breach. While there are steps we can take as consumers to protect ourselves, sometimes we can't control when a company that promised to protect our personal data gets hacked.

In 2023, Statista reported that 52% of all global organization breaches involved customers' personal identifiable information (PII), making your personal data – addresses, numbers, names, birth dates, SSNs, etc. – the most commonly breached type of data. A recent example is ChangeHealthcare, breached in February of this year. Due to the breach, it's estimated that one-third of Americans – possibly including you – had sensitive information leaked onto the dark web.

So now what? What do you do when you receive a letter in the mail from your health care provider or favorite retail store admitting, "Whoops, we got breached." It's more than upsetting to think that your data is now in the hands of criminals.

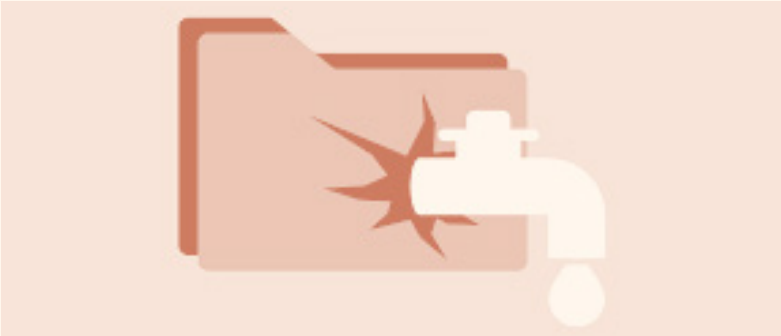
When sensitive information leaks, you'll have to do some recon to protect your accounts from suspicious activity. Follow the seven steps on the next page to stop the bleeding after a company fails to protect your data from being compromised.

What To Do After Your Data's Been Leaked

1. First, make sure the breach is legit.
One ploy that hackers use to get our data is to impersonate popular companies and send out fake e-mails or letters about an alleged breach. Whenever you get a notification like this, go to the company's website or call the company directly. Do NOT use information in the letter or e-mail because it could be fake. Verify that the company was hacked and which of your data may have been compromised. Try to get as much information as possible from the company about the breach. When did it happen? Was your data actually impacted? What support is the company offering its customers to mitigate the breach? For example, some companies offer yearlong free credit monitoring or identity fraud prevention.

2. Figure out what data was stolen.
After speaking directly with the company, determine what data was stolen. Credit cards can be easily replaced; Social Security numbers, not so much. You'll want to know what was compromised so you can take the necessary steps to monitor or update that information.

3. Change passwords and turn on MFA.
After a breach, you'll want to quickly update to a new, strong password for the breached account and any account with the same login credentials. Additionally, if you see an option to log out all devices currently logged in to your account, do that.



While you're doing that, make sure you have multifactor authentication turned on in your account or privacy settings so that even if a hacker has your login, they can't access your account without your biometric data or a separate code.

4. Monitor your accounts.
Even after changing your passwords, you should keep a close eye on any accounts linked to the breach. Watch out for any account updates or password changes you didn't authorize. They may be a sign of identity theft. If your credit card number was stolen, pay attention to your bank and financial accounts and look for unusual activity, such as unexpected purchases.

5. Report it.
If you're not sure a company knows it's been breached or you've experienced fraud due to a breach, report it to relevant authorities like local law enforcement or the Federal Trade Commission. They can provide guidance and next steps on how to protect your identity.

6. Be aware of phishing attempts.
Often, after data leaks, hackers use the information about you they stole to send you phishing e-mails or calls to trick you into giving away even more sensitive information. Be very wary of any e-mails you weren't expecting, especially those that request personal or financial information, and avoid clicking on any links or attachments.

7. Consider identity theft and data breach protection.
Consider identity theft protection after a breach, especially when highly sensitive data is stolen, like your SSN. It's a time-consuming process to replace a Social Security card. In the meantime, criminals could be using it to impersonate you. Identity theft and data breach protection help monitor your credit or other accounts, protect your identity and notify you when your data appears on the dark web.

While companies are responsible for protecting customer information, breaches can and will still occur. By following the steps above, you can minimize a breach's impact on your life. Ultimately, we must all contribute to protecting our information in an increasingly risky digital world.

RJ2 Technologies can help you prevent malicious breaches and protect your business. Call **(847) 303-1194** today for more information.

RJ2 UPDATES

Vendor Partner Highlight

RJ2 Technologies is happy to announce a product addition to their IT Stack, QVerify with CyberQP - a leading provider of Privileged Access Management solutions designed for Managed Service Providers (MSPs). The CyberQP platform equips MSPs with the software they need to manage multiple client admin accounts across tenants, regularly rotate passwords for critical accounts, verify client identities and mitigate risks on your attack surfaces, all through one intuitive dashboard.

CyberQP

QVerify is built specifically for MSPs with the advanced security and management features to handle clients at scale. This provides proactive solutions to protect against modern social engineering techniques or impersonation attacks, safeguarding our help desk with native intergrations into our current systems. By adding QVerify to RJ2's IT Stack, this will increase efficiency by using the mobile app, SMS, email, or a mobile device. QVerify helps RJ2 as we are able to easily verify the identities through the identity verification app, secruly and quickly unlocking accounts and resetting passwords.

RJ2 Technologies, a leading managed IT support provider that has supported its clients for over 20 years, has this strategic partnership with CyberQP to offer a crucial layer of security for the information that matters to their clients, and to verify and protect end user identities. This collaboration is a vital component of RJ2's offering going forward, ensuring that their clients are protected by a security-focused Privileged Access Management firm and allowing RJ2 Technologies offer even better services to our customers. To learn more about this collaboration between RJ2 Technologies and CyberQP, **call (847)303-1194** for more information.

The Digital Art of Saying "Thank You"

In today's digitalized world, showing gratitude goes beyond a simple e-mail. Video messages, personalized with tools like Cameo or Loom, offer heartfelt thank-yous that resonate. E-gift cards tailored to recipients' interests or even digital badges or writing endorsements for employees on platforms like LinkedIn can make appreciation tangible.

Gamified employee recognition systems, like Secchi, and gamified customer reward programs where customers earn points or badges for milestones, foster engagement and gratitude simultaneously. In our modern hybrid workforces, sometimes we can't say "thank you" in person, but by embracing the power of digital tools, we can reimagine our expressions of thanks in 2024, blending warmth with technology.

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

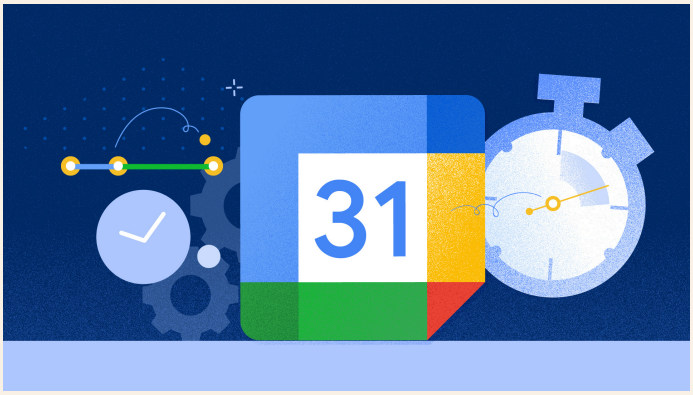
@RJ2Technologies

@RJ2Technologies532

Reading Corner

Are You Using This Helpful Google Calendar Hack?

It's a bit embarrassing when you log in to your computer at 9:00 a.m. only to realize you missed the all-team Zoom meeting at 8:30 a.m. Thankfully, Google Calendar offers a helpful hack: daily agendas. With this feature, you can send yourself a daily agenda first thing in the morning so you know everything planned for the day. To set it up, log into your Google account and go to Settings. Find "Settings for my calendars" > "Other notifications" > "Daily agenda." The default is set to "None," so click on it and change it to "Email." Now you have a daily agenda automatically sent to your inbox before you even get out of bed!



Don't Make This Mistake with Your Home's Smart Tech

Smart devices are so pervasive throughout our homes that it's hard to imagine what life was like before them. From door cams that show us when our kids get home to AI-powered devices that keep track of grocery lists and play our favorite music while we cook, we truly live in "smart" homes.
But unlike devices of the past, you can't "set and forget" smart devices. These tools are connected to the Internet, where hackers keep a close eye out for unprotected devices. When they find a device with a weak password, they can access it and carry out terrifying crimes like watching your family through a home camera. Before you plug in your smart device, follow these simple steps to make sure it's not an open door for peering eyes.

Pros And Cons Of Smart Devices

When hackers find an unprotected device – like an indoor cam that you never bothered to change the default password to – they can access sensitive information on your account, including your address, birth date, e-mail address and phone number. Criminals use this information to create a profile about you and carry out targeted attacks. A family in Mississippi even had a hacker taunt their young daughter through their ring camera. Thankfully, you can take a few simple security steps to avoid becoming a victim of your smart device.

Steps To Keep Your Smart Home Safe

1. Change the default login information immediately. Default passwords are low-hanging fruit for hackers, so be sure to change this to a new, stronger password right away.
2. Make sure your WiFi is secure. If your WiFi password is a few years old or you use the same password on other accounts, change it to a stronger password.
3. Enable multifactor authentication (MFA) in security settings. This way, users can only log in with a security code or authenticator app, making it nearly impossible for hackers to get in.
4. Regularly update the device. Updates fix issues or add new features that may improve your security. Don't skip these updates. If your smart device doesn't update automatically, set a reminder in your phone to check for updates periodically.
5. Consider separate networks. Many WiFi providers offer guest networks. Consider connecting smart devices to a home guest network separate from the one that your phones or laptops are on. This way, if a smart device is hacked, it's not a straight shot to devices holding more valuable information.

The biggest mistake smart-device users make is thinking they can plug in their devices and walk away. These tips go a long way toward ensuring that your device isn't an open door to creepy criminals.

Recognizing Excellence

Employee Recognition

Here at RJ2 Technologies we recognize those who put in hard work and dedication not only towards our services, but to the teamwork they build amongst themselves.

Richard Brohammer - Senior Systems Engineer

Richard has been in IT since 2011, joining RJ2 in May of 2024. He is hyper focused on client support and enjoys getting his users up and running securely and effectively. Richard grew up on military bases in Germany and moved to the US when his father retired in 1991. He started his IT journey with old Army hand-me-down technologies.

In his spare time, he enjoys making food and drinks, creating beers and meals, and experimenting with the old ways of fermentation and preserving foods.

5 Tech Tips to Help Improve Productivity While You Work From Home

Working from home presents several challenges that people commonly face. Home environments can be full of distractions and remote work can lead to feelings of isolation and poor collaboration. Without the structure of an office, staying motivated can be challenging. Follow these 5 tech tips to help you improve your productivity while you work from home.

1. Use Collaboration Tools
Leverage tools like Microsoft Teams, Slack, or Zoom for seamless communication with colleagues. These platforms facilitate virtual meetings, chats, and file sharing, helping you stay connected with colleagues and remove the feeling of isolation.

2. Backup Your Data
Avoid the stress of losing your data by regularly backing up your work files to the cloud. Services like OneDrive, Google Drive, or Dropbox can help protect your important documents.

3. Set Up Virtual Private Networks (VPNs)
If your work involves sensitive data, use a VPN to secure your internet connection. It encrypts your online activity and ensures privacy.

4. User-Friendly Accessories in Dedicated Workspaces
Invest in a user-friendly keyboard, mouse, and chair. Proper posture and comfort are essential for long hours of work. Create a dedicated workspace and establish boundaries with others in your household.

5. Stay Active
Take short breaks throughout the day to stretch, walk, or do light exercises. Physical activity boosts energy levels, reduces stress, and enhances focus. Consider using apps or reminders to prompt movement to avoid overcommitting to tasks and overworking yourself.