ISSUE 21 FALL 2019

RJ2 TECHNOLOGIES

Newsletter

What's Inside

Cloud Migration Tips for Unified Communications

With the increased popularity of cloud technology, the productivity benefits of cloud-based unified communications (UC) are well-known. But organizations migrating UC to the cloud must realize that its performance relies on a number of factors. If you're considering moving your UC to the cloud, follow these tips.

OPT FOR A GRADUAL TRANSITION

Migrating unified communications to the cloud doesn't have to be accomplished in one big move. It can be done gradually. You can move UC for departments that can benefit from it, while those with no pressing need for a cloud-based UC, such as a company's call center, can keep using on-premises systems. This way, users can ease their way into the new system without experiencing network disruptions, which could lead to reduced productivity.

SECURE SUFFICIENT BANDWIDTH

Issues on speed and performance will inevitably arise, so make sure to cover all the bases before migration. That means securing a reliable internet service provider, checking the stability of your internal network, and having a Plan B. This is a critical point to ponder if you have operations in locations where unstable or slow networks could pose serious problems. Determine the level of bandwidth your entire business needs, and get it from an ISP that can deliver.

TEST, TEST, TEST

Transitioning UC to the cloud may appear seamless, but there may be a few unexpected kinks that need ironing out long after the migration is declared a success. To soften potentially costly and time-consuming impacts, test the systems throughout the duration of the migration. Whether you're trying out voice, data, or video, conduct tests, set benchmarks for performance, and predict future usage patterns.

GO LIVE AND ACT ON IDENTIFIED PROBLEM POINTS

After going live with your cloud UC, consider the overall user experience and availability of support for devices, applications, and other components. Are persistent connectivity issues going to cause troublesome conference calls? This and other issues may prove detrimental in the long run so keep them in mind when deciding to keep, enhance, or discontinue a cloud-based UC. Cloud migration should solve problems, not cause them.

CONSTANTLY MONITOR PERFORMANCE AND QUALITY

Don't be surprised if you encounter a few issues even after extensive testing. Migrating to the cloud simply requires planning and a sustainable strategy, whether your organization is dependent on instant messaging, voice conferencing, or video you will be working with several vendors, so always demand for the best service.

Having your UC moved to the cloud may seem like a daunting move. But with our cloud technology and VoIP know-how, we'll make sure it's an easy process. Contact us today for advice.

Contact RJ2

(847) 303-1194

Corporate Office
1900 East Golf Rd.
Suite 600
Schaumburg, IL 60173

Chicago Office
333 S. Wabash Ave
Suite 2700
Chicago, IL 60604

Protecting your Facebook and Twitter from Hackers

T***he Facebook worldwide privacy scandal*** should have been a wake up call for all of us to revisit our social media privacy settings. We should be vigilant in keeping our personal information safe. Here are tips to keep your Facebook and Twitter accounts well-secured.

Lock screens exist for a reason

Lock all your computing devices as soon as you stop using them. This way, you are safe from the simplest hack of all: someone opening a browser on your computer that has your social media login saved.

Strong passwords are never out of fashion

Unlocking your phone may be limited to a six-digit passcode, but you'll need something much more complicated for your account password. Create a password that you don't use for any other account because with the regular occurrence of data breaches, hackers probably already have a long list of your favorite passwords from other websites and platforms.

It is best to use a password manager like an app or online service that allows you to generate and retrieve complex passwords.

You can also enable two-factor authentication, which requires a secondary verification step such as a code sent to your phone. Even if hackers have your password, they won't be able to log in without your phone.

Make use of social media features

Facebook can help you keep tabs on who's accessing your account and from where. Click on the down arrow located at the upper right corner of your Newsfeed and select Settings. Then click Security and Login to get more information. If you sense an imposter, click the right-hand icon so you can log out remotely or report the person.

From there, turn on Get alerts about unrecognized logins to get notifications via Facebook, Messenger, or email if someone is logged into your account from an unrecognized browser. Unfortunately, Twitter doesn't have the same option (which makes two-factor authentication extremely necessary).

Hackers can also barge into your Facebook and Twitter accounts through third-party services that you've given access to your profiles, so make sure to double-check what you have approved.

Facebook: Go to Settings > Apps and Websites to view and manage outside service with access to your account
Twitter: Go to Settings and Privacy > Apps to check and edit the list

Lastly, be sure to check the permissions Facebook and Twitter have on your smart phone or tablet.

Android: Go to Settings > Apps > App permissions
iOS: Go to Settings > Privacy to manage which service can access which parts of your phone

Less personal info, fewer problems

These steps are just the beginning of what you should be doing. You should also limit the personal data you input into your social media accounts. Avoid oversharing.

By following these tips, you can prevent Facebook and Twitter hacking. Cybersecurity is a sprawling issue and social media privacy is such a small sliver of what you need to stay on top of. For 24/7 support, call our team of experts today.

FEATURED PARTNER

Huntress

Security Detection Service

Huntress partners with MSPs to detect threats which slip past anti-virus. With managed breach detertion, customers remian productive while remaining profitable.

RJ2 SPOTLIGHT

Ernest Wegiel

Support Engineer

Ernest Wegiel has been in the professional field since 2008. He is a Network Communication graduate from DeVry University – Chicago. Ernest started his career as a Wedding Consultant at Richard Remiard Event Design. Before joining RJ2 he was a Tier 1 Support Engineer at Rkon located in Chicago IL.

Ernest joined RJ2 Technologies as a Support Engineer in 2017. His duties are to diagnose and troubleshoot software, hardware, data backup and network problems.

Fun Fact: Ernest holds a Brown Belt in Martial Arts.

BUSINESS PRESENCE

How to Delete Data from Your Mobile Device

It's not our business if you want to sell your old smart phone or give it away. But it's a good idea to securely delete what's stored in it because you wouldn't want the next owner to get hold of your sensitive information. Follow the steps below before letting go of your device.

1. ENCRYPT YOUR ANDROID PHONE

Ensure that strangers don't have access to your private data by encrypting it to make it unreadable. Newer phones usually encrypt data by default. But if you're unsure about yours, double-check to avoid regrets later.

Go to Settings in your phone and search for Encryption. Where you'll find that depends on the phone you're using, but it should be easy to locate. Once there, you'll see whether your device is encrypted or not. If it's the latter, start the encryption process. This normally takes an hour or more, and you can't use your device during that time.

2. REMOVE THE SIM AND STORAGE CARDS

Now that your data is encrypted, remove your SIM card and external memory card. Both are linked to your identity and contain sensitive information so don't let them out of your sight.

3. PERFORM A FACTORY RESET

You can now start the actual data wiping process. Under Settings, look for Backup & Reset and go to Factory Data Reset. This is where you can remove data and accounts from your phone. You will be asked to verify your fingerprint, or input your password, pattern, or PIN before starting the process.

4. SEVER TIES TO SPECIFIC WEBSITES

The final step is to manually remove your old device from Google and other websites it is associated with. Go to the concerned sites, choose your device, and remove it from the list of Trusted Devices. Don't forget your password manager and multi-device authentication apps; sign in to those and close any connections there as well.

As long as you follow these four easy steps, you can safely get rid of your old mobile phone. For those who are still worried about their data, give us a call. We'll protect your files from prying eyes and give you valuable tips to secure your Android device.

Featured Product

Huntress Protection Agent

Our partners have deployed Huntress to hundreds of their clients in less than 10 minutes using their existing Remote Monitoring and Management (RMM) software.

We've built our endpoint agent to seamlessly integrate into the work flows MSPs know and expect. After deploying our software, our partners return to the tasks that support their customers and grow their businesses. When our managed detection service discovers a breach, we create a detailed remediation recommendation directly into their existing ticketing system. No need to hire cybersecurity rockstars. No extra pane of glass to monitor.

September

"Any sufficiently advanced technology is indistinguishable from magic. "
-Arthur Clarke

Tech Tip of the Month:
September is National Disaster Preparedness Month! Are you prepared?

5 Things to do to Protect Your Business:

1. Review Your Business Insurance
2. Consider Cloud Computing
3. Secure Your Data
4. Write a Simple Disaster Recovery Plan
5. Review Your Employee Internet Policy

Call RJ2 today at 847-380-3430 to get started!