Total Networks
Business IT Done Right

NetworkNews

February 2018

This Issue:

Hitman Email Scam Threatens Your Life, Instead of Your Data

Email scams have become a sort of punchline, often featuring Nigerian princes or wealthy, unknown relatives in need of funds to get home. However, another email scam is anything but amusing, as it uses a unique possession of the target to entice them to comply: their life...

Read the Rest Online!
http://bit.ly/2rcqZiH

About Total Networks

Locally owned and operated since 1986, Total Networks is the only firm in Arizona to receive CompTIA's Security Trustmark validating the firm's adherence to best practices for information security. Services include IT support, security & compliance assessments, document management, backup & disaster recovery and IT planning/CIO services.

Visit us **online** at:
totalnetworks.com

Customer Service Success Story

Carrie Valenzuela, Firm Administrator
Carrie is the Firm Administrator for a Valley law firm. They've been clients with Total Networks since early 2016. She was gracious enough to take time from her busy schedule to talk about their experience in partnering with Total Networks for managed services. Here's what Carrie had to say:

Prior to working with Total Networks, what was your service experience like with other IT providers?
Prior to this firm, my experience was with in-house IT departments. Total Networks can respond faster and with less push-back than most in-house departments. When contacting Total Networks, I feel like a valued client and that makes everything easier.

What benefits, or value has your firm seen in partnering with Total Networks?
Having someone available 24/7 has been amazing! I appreciate that Total Networks takes a proactive approach to our company's IT needs. For example, the continuous monitoring is wonderful and Total Networks has notified us of potential issues before they become problems.

Would you recommend Total Networks services to others?
I would recommend Total Networks managed services to anyone. We merged with another firm and added a second physical office. We would not have been able to meet the short timetable to make things happen without Total Networks. **http://bit.ly/2Bcpz7q**

There are New Ways to Secure Your Data

Security is an aspect of running a business that absolutely cannot be ignored, regardless of whether or not you see it as a considerable issue in the near future. The fact remains that your organization will always be at risk unless you take actions to keep it safe today. By taking advantage of some of the latest and greatest security tools on the market, you'll be able to protect not only from the basic threats, but more advanced ones as well.

No matter how advanced technology becomes, it can fall victim to even the most basic of threats if left unchecked. Your desktop workstation is certainly not immune to threats like viruses, malware, spam, and so much more, and even the most vigilant business could expose its infrastructure to these common threats. Since consumer-grade services are likely not strong enough to protect your business's important data, you'll need to turn to enterprise-grade solutions that can be tricky for small businesses to afford.

One of the greatest ways you can protect your organization is by implementing a Unified Threat Management tool that fulfills the roles of various security solutions in one convenient package. For example, you could implement an enterprise-grade antivirus and firewall to keep threats out of your infrastructure and promptly eliminate those that do infiltrate your defenses. Furthermore, preventative solutions like spam protection and content filtering can limit your organization's exposure to threats in the first place, which saves time and money in the long run.

(Continued on page 3)

Where the Internet Stands in 2018

People spend a lot of money on the Internet. From an individual standpoint, the amount the average person spends on Internet-based services is their largest expense outside of the money they spend on their residence, and perhaps their transportation costs. In order to understand the landscape of what is effectively a battle for Internet supremacy, you first have to take a look at the battlefield itself.

As of September, of the 7.5 billion people on the planet, nearly 3.9 billion of them (51.7%) use the Internet. In North America, 88.1 percent of people (or roughly 320 million) use the Internet in some fashion. This presents opportunities for thousands of companies. Some provide Internet access to would-be consumers. Some deliver content services. Some deliver applications, computing storage, or processing. This has led to the marketing boom you see on the Internet today; and, is where you find a battle raging between the demand created by billions of consumers, and the companies that deliver the services needed to access that customer base.

A lot of questions have been asked recently about what the Internet is. Questions like:

- How do you monetize access to billions of potential customers?
- Should Internet access be free?
- Is Internet access a utility (and thus governed by different rules)?
- Who is in charge of the Internet?
- What is the Internet of Things?

Questions like these produce a variety of answers. With the smoldering embers of the U.S. net neutrality laws suggesting further corporate control of the Internet, we'll look at the way the Internet is set up in 2018, the costs for businesses and individuals, and why the companies that control access to the Internet are licking their proverbial chops; and, how it challenges the core interpretation of what exactly the Internet is.

The Internet in 2018

The Internet has come a long way in a short time–so far it seems, that it's hardly recognizable. The Internet of 2018 will continue to be the predominant marketplace in the world. It is seemingly in the process of being consolidated. In fact, 50% of Internet traffic in North America is from 35 websites. In 2007, that same amount of traffic was spread around several thousand...

Read the Rest Online!
http://bit.ly/2rcLgVs

Is Your Business Considering Moving to Managed IT?

Your business relies on its technology being maintained properly, but it's not always as simple as updating a software application or replacing a hard drive following a catastrophic failure. You have to think about who you're paying to maintain your technology solutions, if there's anyone doing it at all. You need to consider what happens when you lose data or when your organization experiences downtime. How do you keep technology from becoming a hindrance for your business?

Managed IT is one of the best ways your organization can capitalize on its technology without worrying about whether or not you're maintaining it properly. The ideal way for a small business to manage its technology is to have professionals handle it while you focus on other aspects of the management process.

In other words, let's ask you a question; is your business running as smoothly as possible? Can you honestly say that you have time in your day to handle multiple technological troubles, as well as all of your other responsibilities? Upper-level executives like the CEO and COO have other responsibilities that are more pressing, and as such, technology maintenance is often left to your employees, who may (or, more likely, not) know what they're doing. Technology maintenance is something that should always be done by professionals, as...

Read the Rest Online!
http://bit.ly/2rei3JB

Do You Have a Unified Strategy to Your Business' Communications

Communication is one of the cornerstones on which your business functions, and without it, you will find that going about your daily duties is considerably more difficult. Communication is one of the many ways your organization accomplishes both major and minor tasks, so you want to pay especially close attention to how your business handles phone calls, email, and even mobile devices– both in and out of the office.

Unified communications include several solutions that your organization can use to stay connected, including a unified email solution, mobile device strategy, and a telephone solution. All of these types of solutions should be built around today's expectations of mobility and flexibility. Here are some of the ways your business can build out a unified communications system that improves connectivity.

Email

Email has long been a staple of business, but how do your employees use it? Do they access it on multiple devices? Do they use the same email service (Hint: They should)? An employee who prefers Gmail over Microsoft Outlook might decide that they would rather use the solution they are most comfortable with. This is an issue, as it spits in the face of your attempt at unified communications.

Email is most useful when it's kept to your preferred email solution, so you should ensure that your organization is prepared to spend time on training employees how it works. The solution you choose should be one that can be used on several different devices so as to provide your employees with maximum choice in how they use the email system. If you're worried about hosting your email server, Total Networks can help you out with that, too.

Mobile Device Management

Mobile devices are all over the place now, and your business could benefit from having them become a part of your infrastructure. However, they need to be managed properly, as the more apps have access to your business's data, the more exposure it gets to potential threats. You need to make sure that you're prepared to handle this influx of mobile devices if you're hoping to provide a truly unified communication infrastructure for your organization.

Beyond compatibility, you want to make sure that your organization is prepared to handle lost or stolen devices, fraudulent apps, and other security risks. Total Networks can help you whitelist and blacklist apps, as well as remotely wipe lost or stolen devices. This helps you keep your data as safe as can be.

Unified Voice over IP

Traditional telephone solutions don't take the flexibility of the modern business in mind. Landlines tend to bundle together services with little flexibility, leading to organizations overpaying for services that they don't need. If you're paying for services that you don't need, you're wasting assets that are better spent elsewhere. Furthermore, you're limited to taking calls on your work phone in your office, hampering your ability to be productive while out of the office or on a business trip.

A Voice over Internet Protocol (VoIP) application is one of the best solutions an organization can implement, as they often work across multiple types of devices and work from a shared database of contacts. Your workers will always have access to client information, even when they aren't in the office. Employees have the option of using their smartphone, desktop, or traditional handset. Having VoIP makes using Unified Communications so much easier for businesses. To learn more about unified communications solutions, reach out to Total Networks at (602)412-5025.

Share this Article!
http://bit.ly/2mLm57C

There are New Ways to Secure Your Data

(Continued from page 1)

More advanced security protections, however, are certainly important for your business as well. Some of the more powerful measures include two-factor authentication and biometric scanning. Two-factor authentication is particularly important, as it provides a secondary credential that must be used to gain access to important information and accounts. Basically, it forces hackers to do even more work to break into an account, as they would have to physically steal your smartphone or other device to which the secondary credential is being sent to, all just to access an account and maybe find something useful.

Biometrics, on the other hand, are a bit harder to fake. Using fingerprint scanners or iris scanners make it considerably more difficult to unlock devices. A hacker would basically have to have the exact same fingerprint or iris as you, so unless there is some incredibly shady business going on, they won't be able to access your devices.

How does your business secure its sensitive information and data infrastructure? Total Networks can help your business avoid considerable security troubles. To learn more, reach out to us at (602)412-5025.

Share this Article!
http://bit.ly/2mK5rVZ

Do You Know What Your Android Permissions Actually Mean?

Downloading an application on an Android device is fairly simple: access the Google Play store, find the app you want to download and press the button that says install. However, it is also too easy to simply hit 'Allow' once the app starts asking for ambiguously-worded permissions. Today, we'll examine what these permissions actually mean.

It is important to understand that these permissions are not ambiguous by accident. Due to the various responses that different users will have to a request to access certain parts of the device (like the camera, for instance), developers have taken to describing the possible effect of an application's access, instead of simply saying what it will be accessing.

Therefore, you may find yourself giving your applications permission to access and even alter more than you realized, simply because the permissions your apps have requested didn't give you a clear idea of what they entail. This can be risky, especially if the app in question was created by an unscrupulous developer seeking access to your information.

If you see the following permission requests, know that they are considered and classified as "Dangerous." The reasons that these permissions could put your security at risk are included.

Phone permissions — These permissions give an app the ability to interact with your calls and call history however the developer wants it to. As a result, the app can make calls (including those that use Voice over Internet Protocol, or VoIP), as well as read and edit your calls list. An app with these permissions can also read your network information to collect data on the calls that you have made, and can even redirect your calls or hang up the phone. Essentially, phone permissions give an app control over the primary function of a cellular phone. While this may sound frightening, it is important to realize that this permission is often asked for so that any app you may be using when you receive a call can be paused. As a result, this is a permission that many games and multimedia apps will ask for.

- **SMS permissions** — These permissions give an app the ability to both send SMS messages and read any that are incoming. Not only does this present some obvious privacy concerns, it also means that a criminal could leverage this access to add paid services to your account without your consent.
- **Contact permissions** — As with any of the permissions on this list, there are completely aboveboard reasons that an application would require access to your contacts, as well as the ability to edit them. However, in the wrong hands, your contact list becomes a resource for a spammer to pull their next victims from. It is also important to consider that these permissions grant access to any accounts that your apps use, including Facebook, Google, and others.
- **Calendar permissions** — With these permissions granted, an app can read, edit, and create events in your calendar. However, this also means that an app can review your calendar without restriction, with the ability to edit or remove anything they want.
- **Camera permissions** — These permissions, perhaps obviously, allow an app to utilize your phone's built-in camera to capture images and video. However, these permissions don't specify that the app has to necessarily be in use to do so, allowing the app to...

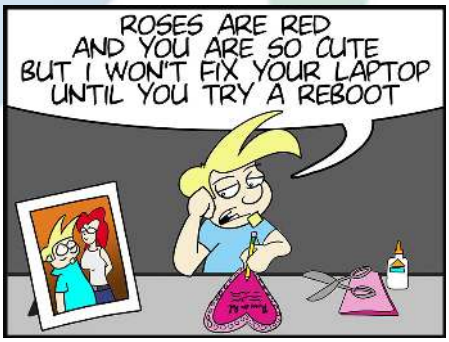
Read the Rest Online!
http://bit.ly/2rdCmXK

We work together with our IT Managed Services clients to jointly create and maintain an up-to-date, effective written technology plan and budget.

If you would like to receive an electronic version of our newsletter please email skinsey@totalnetworks.com

Dave and Stephanie Kinsey
Owners

Bill Fox
VP, Client Services



Total Networks

4201 North 24th Street
Suite 230
Phoenix, AZ 85016
Voice: 602-412-5025

Visit us **online** at:
totalnetworks.com

info@totalnetworks.com
facebook.totalnetworks.com
linkedin.totalnetworks.com
twitter.totalnetworks.com