Total Networks
Business IT Done Right

NetworkNews
March 2018

This Issue:

Targeted Ransomware Checks for Particular Attributes

Put yourself in the shoes of a cybercriminal. If you were to launch a ransomware attack, who would be your target? Would you launch an indiscriminate attack to try to snare as many as you could, or would you narrow your focus to be more selective? As it happens, real-life cybercriminals have largely made the shift to targeted, relatively tiny, ransomware attacks...

Read the Rest Online!
http://bit.ly/2EO1mYA

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

5 Cybersecurity Tips to Protect Your Business

The majority of data breaches happen to businesses with less than 100 employees. Cybercriminals often target small and midsize businesses, because they tend to spend less on cybersecurity than larger organizations, which makes them an easier target. Your firm likely collects valuable data such as client, employee and vendor names, addresses, social security numbers, dates of birth, driver's licenses and insurance information. This information is everything a criminal needs to commit identity theft and other cybercrimes.

Ransomware is a real threat to all businesses.

Ransomware is a method of holding data hostage until a ransom or payment has been made to release the data. Ransomware is usually associated with fake emails called phishing emails that may contain dangerous links or malicious attachments. The email is "phishing" for a click so that it can silently launch a program to lock all the data the clicker has access to by encrypting it. Once the program encrypts everything it can, it will display a message extorting money for the promise of a key.

Criminals are targeting law firms and other businesses that have valuable data they cannot afford to lose. The risk of being caught spreading ransomware is much lower than traditional hacking or cybercrime. There are firms that have been shut down for weeks as a result of successful ransomware attacks that have encrypted the entire network and made access to

(Continued on page 2)

What is the Weakest Link in Your IT Network?

Today's computer operating systems and software have more sophisticated built-in security than ever before. In most organizations, however, the people using these systems lack the knowledge to cope with the ever more sophisticated threats which target your valuable data. In fact, now the majority of malware infections are a direct result of social engineering ploys leveraged by hackers.

Social engineering involves manipulating employees in order to access company systems and private information. According to the IBM Security Services 2014 Cyber Security Intelligence Index report, 95% of breaches are caused by human error. For cyber criminals, it is the easiest method for obtaining access to a private company system.

Employee awareness of social engineering tactics is essential for protecting your firm's data. Here is an overview of common scams to educate your staff.

Six Common Types of Social Engineering Scams:

1. **Phishing** – this is the leading tactic leveraged by today's hackers. The primary way phishers will strike is by email, but they can also be delivered in the form of chat, website ads and website impersonations. Phishing is effective by creating a sense of urgency or fear to induce a response. Always be wary, and never reply to emails from senders that you don't recognize. These emails often go directly to your spam folder, so be especially careful of releasing messages from your quarantine. One incorrectly identified phishing email is all it takes to infiltrate a business. McAfee conducted a quiz of 30,000 business users in 49

(Continued on page 3)

3 Types of Software and How Businesses Use Them

For the modern business owner or executive, making smart business decisions has become a necessity. Margins are small, efficiency is key, and if we were to be completely honest, business is a day-in and day-out grind. In the course of doing business much is made of cost reduction and curtailing inefficiencies that lead to wasted capital. Much is made of collaborative systems that allow for remote access. Much is made of protocol, process, and performance. With so many moving parts in every business, there has to be the "glue" that allows for cohesive actions to be taken. That "glue" is software.

IT is a multi-trillion dollar business ($3.5 trillion in 2017 according to Gartner), and enterprise software, that is the software that businesses use to conduct business, makes up for around a tenth of it, at $351 billion. Any way you slice it, software is a significant expense for most businesses. This month, we are going to take a look at the types of software that businesses use most, what they use it for, and how to decide a certain software works for your business.

For our purposes, we will split the software businesses use into three separate categories. They are security, operations, and relationships.

Security Software

We'll start with security software, since without it, you may not even need the other two types. Security software is, as the name suggests, the software you use to keep your organization's computers free from threats. Any computer with an operating system will have some security built in, but for a business, you are likely going to need more, and in some cases, a lot more.

The first thing you'll need to know about security software is that you are in danger. Your data is being targeted by innumerable entities that are looking to steal it from you for their own gains. In fact, for every threat that is developed to breach network security, there has to be a solution created that mitigates it. This fact has led to a massive security market in which consumers, even the IT-savvy ones, are left overwhelmed and scratching their heads. Some threats include:

- Ransomware
- Phishing
- Viruses
- Malware
- Trojan horses
- Denial of service (DDOS)
- Hackers
- Human error
- Sabotage
- And more…

Conversely, if you are able to stop these threats before they get into your business' computing network (or onto the PC where you do your business computing), you will have a secure computing environment 100 out of 100 times. This is why it is essential for small business...

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

5 Cybersecurity Tips to Protect Your Business

(Continued from page 1)

company data and systems impossible. Paying the ransom may not work and you don't want to be in that position in the first place.

Best Practices

Employ the following best practices to minimize the chance of data breaches.

1. **Secure passwords.** Passwords are the key to networks, client information, online banking and social media. Password best practices include:

- *Use strong passwords.* The longer the better. Longer passwords are harder for thieves to crack. Include numbers, capital letters and symbols. Require strong passwords via system settings.
- *Consider using passphrases.* When possible, use a phrase such as "I went to Lincoln Middle School in 2004" and use the initial of each word like this: "Iw2LMSi#2004".
- *Don't use dictionary words.* If it is in the dictionary, there is a chance someone will guess it. There is even software that criminals use that can guess words used in dictionaries.
- *Don't post it in plain sight.* This might seem obvious, but studies have found that a lot of people post their password on their monitor with a sticky note.
- *Use multi-factor authentication.* Set up multi-factor authentication that requires you to have your phone or another physical device (at a minimum, when logging into your account from a new device).
- *Don't reuse passwords; consider using a password manager.* Creating very strong random passwords that are encrypted and saved with one master password (and second factor) can significantly minimize your risk.

2. **Encrypt data.** The best way to protect sensitive information is to use encryption. Under many federal and state regulations, encryption is a "safe harbor". This means if a mobile device is lost or stolen and the data is encrypted, then the incident would not result in a reportable breach.

Consider encrypting mobile devices, laptops, USB drives, workstations and email. Without encryption, a stolen device may result in a data breach. Emails could contain sensitive information...

Read the Rest Online!
http://bit.ly/2Eb71qQ

5 Ways a Managed Service Provider Can Help Your Business

How much does your business rely on technology to keep your organization running forward? As business technology becomes more complex, it's becoming increasingly popular for organizations to outsource their IT to a managed solutions provider.

Unlike break-fix IT solutions, which depend on your technology breaking down, managed IT solutions aim to keep your technology in proper working order, as well as take action to proactively treat issues before they become long-term problems. Here are some of the best ways that managed IT can help your organization take better advantage of its technology.

Guaranteeing Flexibility

Let's say that you choose to hire more employees for a specific department of your business. This means that you have more users, which can lead to more software licenses needed, more email accounts to archive, more endpoints to secure, and much more. Basically, as your workforce needs change, so too must your managed IT service agreement. Total Networks offers scalable solutions that can be customized to fit the needs of your business.

Supplementing In-House Maintenance

Let's say that you do have an in-house technician or a small group of workers dedicated to IT maintenance. They might be able to get most of their work done, but generally speaking, your in-house technicians probably have their hands full or need additional support for projects or to take a vacation. A managed IT provider helps to augment and work with your in-house team to create greater success for your organization as a whole.

Working with Your Vendors

You work with a lot of vendors to give your company the access to the products your organization needs to be successful. This includes hardware or cloud vendors for your workstations and servers, software developers for all of your productivity suite needs, and any other service providers that you have. Reaching out to all of these can be time-consuming, which is why managed service providers like Total Networks offer vendor management services to create a single point of contact to keep your attention on your business and not your vendors.

Improving Operational Efficiency

By outsourcing, you can take advantage of labor-saving monitoring and management tools which are cost-prohibitive for a small business on their own. An in-house monitoring system may not alert anyone if it's located in your office. Total Networks has a sophisticated monitoring system that checks your systems constantly, and technicians who review and respond to alerts every day. An external IT team can monitor your system more closely than any of your staff. This is the key to identifying and correcting root cause issues before they create downtime.

Increased Security and Regulation Compliance Focus

Having a managed service provider is one of the best things you can do for your network security. Our team will help keep your defenses closed against hackers and your security configuration up to date. While your on-site staff can get caught up in daily or seasonal excitement, your outsourced managed IT team will steadily protect and update your network, reliably maintaining solid network security...

Read the Rest Online!
http://bit.ly/2E7ODPf

What is the Weakest Link in Your IT Network?

(Continued from page 1)

countries. Only 6% of the respondents correctly classified all of the emails as legitimate or phishing. 80% of all employees fell for at least one phishing email. If you suspect your message is phishing, hit Alt-F4 or upper-right "X" instead of "Cancel" or "Close."

2. **Baiting** –similar to phishing, baiters entice you to provide information or visit an infected website by offering something alluring in exchange. The "bait" might offer digital content such as a free music or software downloads. A common offline baiting technique is when a branded USB storage device is left in the workplace or a public area for an end user to find. Once the bait is taken, malicious software is delivered directly into the victim's computer.
3. **Pretexting**– is when a hacker creates a false sense of trust with the victim by impersonating a co-worker or a figure of authority within the company. For example, a hacker may send an email or a chat message posing as the head of IT Support who needs private data in order to comply with a company audit (that isn't real). Successful pretexting depends by how well the attacker creates credibility. The attacker may have rate sheets for software they are "selling" and spend time researching your persona to look the part in order to earn your trust.
5. **Quid Pro Quo** – "something for something," occurs when a hacker offers a service in exchange for private data. For example, an employee might receive a phone call from the hacker impersonating an IT specialist offering IT assistance for a bogus computer problem. The criminal might walk the employee...

Read the Rest Online!
http://bit.ly/2E7ZfOe

Managing Gmail with Labels and Filters

Gmail is a great way to take advantage of business email, but do you know all of the ins and outs of how to use some of its finer details? This month's tip is dedicated to going over some of the more useful features of Gmail, like filters and labels– both of which will be helpful in controlling your inbox.

Labels and Filters

Gmail helps you keep your messages organized through the use of labels and filters. Basically, you can assign rules that will apply to any messages that you receive. By effectively using filters, you can make browsing your inbox more efficient, as well as consolidate similar messages with little effort.

For example, a filter could be used to assign a label to any message that holds "quarterly report" in the subject line. These labels would then be applied to any incoming messages that have that specific criteria.

Creating a Filter

To create a filter in Gmail, just follow these steps:

- Click the down arrow in the search bar. You can then select specific details that you want to include in your search criteria.
- Select the criteria that you want your filter to look for. Once you've done so, click on Create filter with this search.
- You'll then be provided with several options, one of which will automatically mark your conversation as important. Be sure to select the option to Apply the label.
- Next, select the drop-down menu that's labeled Choose label. You can then create a new label or one that has already been made.
- Once the filter has been configured, select the Create Filter button.

"Gmail helps you keep your messages organized through the use of labels and filters. Basically, you can assign rules that will apply to any messages that you receive. By effectively using filters, you can make browsing your inbox more efficient..."

Creating a Label

You can also apply labels to your messages, but in order to do so, you first need to make the label. You'll be able to both apply labels as you receive messages, or apply them to existing messages.

We'll walk you through the process:

- In Gmail, click on the More option on the left side of the screen.
- Next, select Create new label.
- Provide a name for your label and create it.

Now all you have to do is apply the label to your messages.

- First, open up the message you want to apply the label to.
- At the top of your screen, select the Label button. You can add a label to any group of messages provided you have selected them all before you click the label button.
- You must then select each label you want to add. You can also create a new label at this point if you need to.

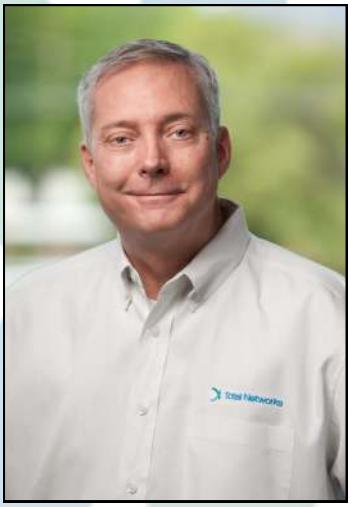
To learn more about how to take full control of your Gmail inbox or to learn about other features of G-Suite, contact us at (602) 412-5025.

Share this Article!
http://bit.ly/2E7zLR5

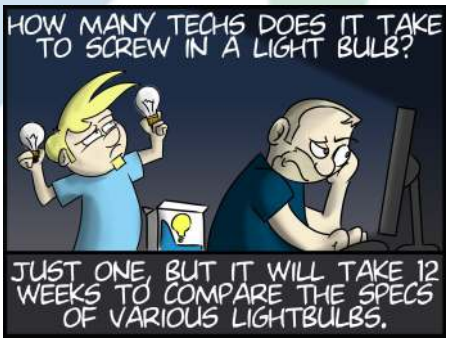
We work together with our IT Managed Services clients to jointly create and maintain an up-to-date, effective written technology plan and budget.

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