TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's New

Don't let your organization be caught like a sitting duck! You've worked way too hard to get where you are today to risk it all due to some little cyberhack you didn't know about. We now have an online based Security Training available for our clients. During the month of September we are giving away 1 month of training for FREE to the first 5 companies that contact us! Call us today at 701-364-2718 or e-mail info@imsnetworking.com.

September 2016

This monthly publication provided courtesy of Rick Johnston, President of Information Management Systems

"Enabling People to Provide Great Products and Services - Anytime, Anyplace, Anywhere"

How To Stay Protected Against Ransomware

Ransomware has become one of the most widespread and damaging threats that internet users face. Since the infamous CryptoLocker first appeared in 2013, we've seen a new era of file-encrypting ransomware variants delivered through spam messages and Exploit Kits, extorting money from home users and businesses alike.

The current wave of ransomware families can have their roots traced back to the early days of FakeAV, through "Locker" variants and finally to the file-encrypting variants that are prevalent today. Each distinct category of malware has shared a common goal – to extort money from victims through social engineering and outright intimidation. The demands for money have grown more forceful with each iteration.

Even though most companies have extensive security mechanisms in place, such as virus scanners, firewalls, IPS systems, anti-SPAM/anti-virus-email-gateways and web filters, we are currently witnessing large numbers of infections worldwide with ransomware infections, such as Cryptowall, TeslaCrypt and Locky. Files on computers and network drives are encrypted as part of these infections in order to blackmail the users of these computers to pay a sum of money, usually in the region of USD 200-500, for the decryption tool.

Why are ransomware attacks so successful?

The main reasons why these infections are successful are:

1. Sophisticated attack technology

Producers of ransomware operate in a highly professional manner. This includes, among other things, usually providing an actual decryption tool after the ransom has been paid.

Skillful social engineering is employed to prompt the user to execute the installation routine of the ransomware. For example, you may get an email that reads something like this: "If the encoding of the attached Word document seems incorrect, please activate macros. This is done as follows..."

2. Security weaknesses in affected companies

Inadequate backup strategy (no real-time backups, backups not offline/off-site).

Updates/patches for operating system

continued on page 2

and applications are not implemented swiftly enough .

Dangerous user/rights permissions (users work as administrators and/or have more file rights on network drives than necessary for their tasks).

"How do I recognize a phishing email?"

Lack of user security training ("Which documents may I open and from whom?", "What is the procedure if a document looks malicious", "How do I recognize a phishing email?").

Security systems (virus scanners, firewalls, IPS, email/web gateways) are not implemented or are not configured correctly. Inadequate network segmentation can also be included here (servers and work stations in the same network).

Lack of knowledge on the part of administrators in the area of IT security (.exe files may be blocked in emails but not Office macros or other active content).

Conflicting priorities ("We know that this method is not secure but our people have to work...").

Best practices to apply immediately

Backup regularly and keep a recent backup copy off-site. There are dozens of ways other than ransomware that files can suddenly vanish, such as fire, flood, theft, a dropped laptop or even an accidental delete. Encrypt your backup and you won't have to worry about the backup device falling into the wrong hands.

Don't enable macros in document attachments received via email. Microsoft deliberately turned off auto-execution of macros by default many years ago as a security measure. A lot of malware infections rely on persuading you to turn macros back on, so don't do it!

Be cautious about unsolicited attachments. The crooks are relying on the dilemma that you shouldn't open a document until you are sure it's one you want, but you can't tell if it's one you want until you open it. If in doubt, leave it out.

Don't give yourself more login power than you need. Most importantly, don't stay logged in as an administrator any longer than is strictly necessary, and avoid browsing, opening documents or other "regular work" activities while you have administrator rights.

Consider installing the Microsoft Office viewers. These viewer applications let you see what documents look like without opening them in Word or Excel itself. In particular, the viewer software doesn't support macros at all, so you can't enable macros by mistake!

Patch early, patch often. Malware that doesn't come in via document macros often relies on security bugs in popular applications, including Office, your browser, Flash and more. The sooner you patch, the fewer open holes remain for the crooks to exploit.

Keep informed about new security features added to your business applications. For example, Office 2016 now includes a control called "Block macros from running in Office files from the internet" which helps protect you from external malicious content without stopping you using macros internally.

Open .JS files with Notepad by default. This helps protect against JavaScript borne malware by enabling you to identify the file type and spot suspicious files.

Show files with their extensions. Malware authors increasingly try to disguise the actual file extension to trick you into opening them. Avoid this by displaying files with their extensions at all times.

Additional measures to secure against ransomware

Employee awareness/training

In addition to the immediate measures described above , it's important that all employees receive regular IT security training. The success of these measures should also be checked regularly.

Encrypting company data

Suitable encryption of company documents can help to prevent malware from obtaining unencrypted access to confidential documents. This prevents damage caused by the outflow of business-relevant documents.

IT Security Best Practices

Many of the measures proposed in this document are "Best Practices" in IT security and should in fact be long established in the company, just like some other measures that have not been mentioned here, e.g. strong passwords. We recommend regular security check-ups/ health checks to identify potential security deficits and to be up to date when it comes to technical and organizational options for protecting your IT infrastructure.

Ransomware is a very present risk for all organizations, and indications suggest that it is not going away any time soon. It is therefore essential to take immediate steps to secure your organization against this type of attack. By following both the short and longer term recommendations outlined in this document, organizations will take significant steps to protect themselves against ransomware infections.

We encourage organizations to educate their employees of these risks. For the month of September we are giving away 1 month of Security Training for FREE to the first 5 companies that contact us! Call us today at 701-364-2718 or email info@imsnetworking.com.

Shiny New Gadget Of The Month:

FitBark Keeps You And Your Dog Healthy

Do you know how well your dog slept last night? How much nutrition – or exercise – your dog really needs? Whether your pup is being well-cared for at doggy day care?

With FitBark you would know all this, and more, about your favorite canine pal.

Doggy health monitors are nothing new. But, according to hundreds of verified reviews on Amazon, Best Buy, App Store and Google Play, FitBark leads the pack.

FitBark attaches to your dog's collar and shares data with FitBark Explore, a dog health data bank that collaborates with over 20 leading universities and research institutions in North America and Europe to gain a better understanding of dog health.

You benefit from all this data by tapping into what FitBark calls truly unprecedented insights into canine health and data. All toward keeping Fido – and you – on the path to health and happiness.

$59.95 at Fitbark.com.

Schedule Meetings With Microsoft FindTime

The art of organizing a meeting is much like chess. Each player has different possible moves, or availabilities; and it's up to you to strategize which pieces to move where, or which events to schedule (or reschedule) when. The objective is to land on a square wherein all participants can attend, but achieving this goal often demands a tiring and time-consuming process. Fortunately, with the help of Microsoft FindTime, you can arrange meetings efficiently and easily.

Before any meetings take place, you'll need to download Microsoft FindTime first. Fear not, because this Microsoft Outlook add-in is easily downloadable and is 100 percent free. FindTime was developed to help you and your guests do just that — find time! Coordinating all attendees' schedules, FindTime will iron out a time that works for everyone.

Just the thought of having to organize a meeting across your organization can stir up anxiety and elicit a huge sigh… Sigh! Why? On top of handling your own hectic schedule, you're expected to juggle your attendees' schedules as well. This would be the moment when telephone calls start to flood in and emails start to go back and forth, rarely heading toward a unified decision.

Bid adieu to all of that with Microsoft FindTime. Simply compose a new email or reply to an existing one and click the New Messaging Poll at the upper right hand corner. From there, choose the attendees, propose a couple tentative meeting times, and let the voting begin! Once a consensus is reached, a confirmation email is automatically sent to everyone attending.

What makes it even easier is that attendees can take a look at the visual summary that tallies all the votes, and who voted for what times. This lets you see what times the majority of people have chosen, giving you a chance to rework your schedule in advance if and when necessary.

Another plus is that to receive a Microsoft FindTime invitation, your friends and family don't need an email address or even an Internet connection! Participants aren't required to have Office 365 either; only the organizers need to access Office 365. This means that you can reach out to your friends, loved ones, and colleagues to organize your meetings, set up playdates, and even plan surprise birthday parties — the possibilities are endless.

For more info about Microsoft FindTime, feel free to send us an email or give us a call! Our experts will gladly answer your questions. We believe that time is money, and money is the last thing you'd want to jeopardize. Allow us to help safeguard your assets by ensuring that all the time you spend on the clock doesn't go to waste. Every minute counts.

Bits & Bytes

Are you addicted to your work?

To find out, rate yourself 1 to 5 on the following statements. Give yourself a 5 for "often" and 1 for "rarely": a) You think of how to free up more time to work. b) You spend more time working than initially intended. c) Your work helps you reduce feelings of guilt, anxiety, helplessness and depression. d) You get stressed when you can't work. e) You set aside hobbies, leisure pursuits and exercise in favor of work. If you averaged 4 to 5, then you may be at least mildly addicted to your work. Is that a bad thing? Not necessarily. While your well-being requires a certain amount of balance, having the drive, enthusiasm and energy to achieve impossible goals marks many of the most successful entrepreneurs. *-Forbes*

We bet you've never even heard of these new technologies.

1) *Perovskite solar cells* promise to be cheap, easy to install and efficient enough to power entire buildings, large or small. Made with a compound called perovskite, they reach new areas of the light spectrum, thus producing far more energy than current solar technology. 2) *Organs-on-chips* allow scientists to test how drugs impact the body – without putting humans or animals at risk. These micro-sized chips emulate how human organs work. By injecting the chips with drugs, scientists can observe responses such as heart palpitations to predict human responses to drugs and diseases. 3) *Super-smart nanosensors*, tiny enough to fit inside the body could, for example, alert a doctor if a patient starts to show signs of heart failure. *-Inc.com*

Did you know your iPhone could do this?

Respond to texts without unlocking the phone. When you get a notification, swipe left on the message and a blue "Reply" button appears. Just tap it and text away! Take a photo with the volume button. For that ultimate, one-handed selfie, open the camera app and press the "+" button for volume on the side of your phone. Have Siri read your texts out loud. This is a great tool for when your hands aren't free or you're on the road. Press the volume button and hold it. When the beep sounds, tell Siri, "Read my texts." When done reading, she'll ask you what to do with the messages. You can have her reply or read them again. *-Entrepreneur*

You are just minutes away from creating a dazzling design - free.

With these 3 online tools you don't need to pay a pro or buy fancy software. 1) *Canva* templates make easy to create a business card, ebook or info-graphic. Just drag and drop objects until you like how it looks. Add images, tweak colors, swap fonts and voila - You've got a design you can be proud of. 2) Your brand's color palette helps get your message across and can even drive conversions. But getting just the right shade can be tough. Upload your photo to *Pictaculous* and get instant color recommendations and hex codes. 3) *PicMonkey* lets you easily edit, re-color, add borders and text - even insert graphics into your images. *-HubSpot*