TECHNOLOGY TIMES

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

What’s New

Windows 10 Free License Upgrade Expires - July 29, 2016. We are less than a month away from the expiration date for your free license of Windows 10 upgrade (for Windows 7 and 8 users only). After that, the upgrade price for Windows 10 Pro will be $199.

Don’t delay! Contact us today to talk about a Windows 10 Upgrade Readiness Assessment - 701-364-2718

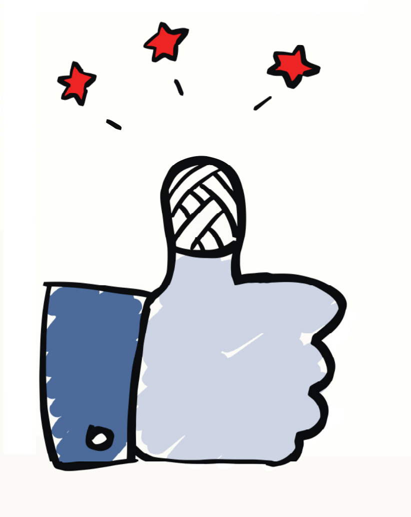
To receive the IMS Upgrade Readiness Assessment for FREE ($420 Value!) You must be one of the first 3 callers!

www.imsnetworking.com/windows10

July 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”



5 Ways To Spot A Social Engineering Attack

“I’m not going to make payroll – we’re going to close our doors as a result of the fraud.”

Unfortunately, that statement is becoming more common among smaller businesses, according to Mitchell Thompson, head of an FBI financial cybercrimes task force in New York.

The FBI reports that since October 2013 more than 12,000 businesses worldwide have been targeted by social engineering–type cyberscams, netting criminals well over $2 billion. And those are just the reported cases. Often, due to customer relationships, PR or other concerns, incidents go unreported.

These unfortunate events were triggered by a particularly nasty form of cyberattack known as “social engineering.”

Social engineering is a method cyber con artists use to lure well-meaning individuals into breaking normal security procedures. They appeal to vanity, authority or greed to exploit their victims. Even a simple willingness to help can be used to extract sensitive data. An attacker might pose as a coworker with an urgent problem that requires otherwise off-limits network resources, for example.

They can be devastatingly effective, and outrageously difficult to defend against.

The key to shielding your network from this threat is a keen, ongoing awareness throughout your organization. To nip one of these scams in the bud, every member of your team must remain alert to these five telltale tactics:

1. **Baiting** – In baiting, the attacker dangles something enticing to move his victim to action. It could be a movie or music download. Or something like a USB flash drive with company logo, labeled “Executive Salary Summary 2016 Q1,” left where a victim can easily find it. Once

continued on page 2

these files are downloaded, or the USB drive is plugged in, the person's or company's computer is infected, providing a point of access for the criminal.

2. **Phishing** – Phishing employs a fake e-mail, chat or website that appears legit. It may convey a message from a bank or other well-known entity asking to "verify" login information. Another ploy is a hacker conveying a well-disguised message claiming you are the "winner" of some prize, along with a request for banking information. Others even appear to be a plea from some charity following a natural disaster. And, unfortunately for the naive, these schemes can be insidiously effective.

> *"The problem with social engineering attacks is you can't easily protect your network against them."*

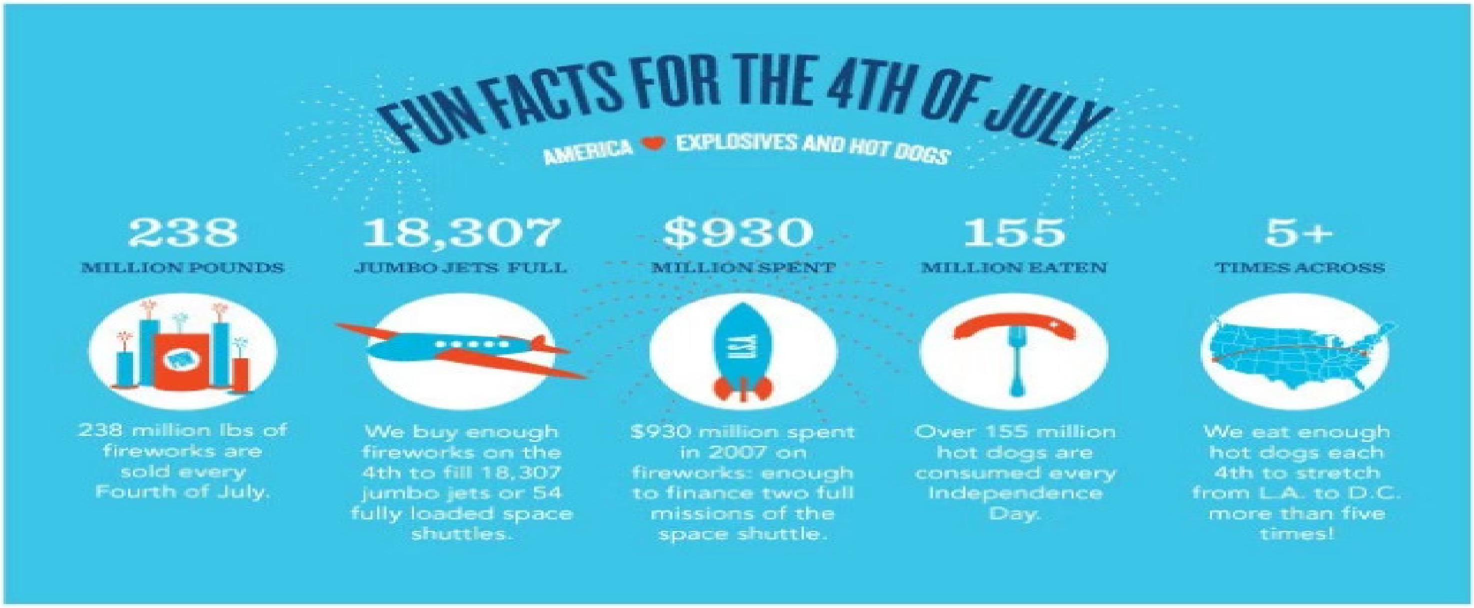
3. **Pretexting** – Pretexting is the human version of phishing, where someone impersonates a trusted individual or authority figure to gain access to login details. It could be a fake IT support person supposedly needing to do maintenance…or an investigator performing a company audit. Other trusted roles might include police officer, tax authority or even custodial personnel, faking an identity to break into your network.

4. **Quid Pro Quo** – A con artist may offer to swap some nifty little goody for information… It could be a t-shirt, or access to an online game or service in exchange for login credentials. Or it could be a researcher asking for your password as part of an experiment with a $100 reward for completion. If it seems fishy, or just a little too good to be true, proceed with extreme caution, or just exit out.

5.**Tailgating** – When somebody follows you into a restricted area, physical or online, you may be dealing with a tailgater. For instance, a legit-looking person may ask you to hold open the door behind you because they forgot their company RFID card. Or someone asks to borrow your laptop or computer to perform a simple task, when in reality they are installing malware.

The problem with social engineering attacks is you can't easily protect your network against them with a simple software or hardware fix. Your whole organization needs to be trained, alert and vigilant against this kind of incursion.

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 July 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.


FUN FACTS FOR THE 4TH OF JULY
AMERICA ♥ EXPLOSIVES AND HOT DOGS
238
MILLION POUNDS
238 million lbs of fireworks are sold every Fourth of July.
18,307
JUMBO JETS FULL
We buy enough fireworks on the 4th to fill 18,307 jumbo jets or 54 fully loaded space shuttles.
$930
MILLION SPENT
$930 million spent in 2007 on fireworks: enough to finance two full missions of the space shuttle.
155
MILLION EATEN
Over 155 million hot dogs are consumed every Independence Day.
5+
TIMES ACROSS
We eat enough hot dogs each 4th to stretch from L.A. to D.C. more than five times!

Shiny New Gadget Of The Month:

Finally: An Easy Way To Control The Family Net

Got kids aged six to 16?

Circle With Disney is a new device that helps make Internet struggles at home a thing of the past. Imagine: no more negotiating with kids to get off the web and come to dinner (or get their homework done).

This 3½-inch white cube with rounded corners (it's not exactly a circle…) lets you control Internet usage around your house with a tap on your iPhone. (Android compatibility coming soon.)

With presets by age group, or custom controls, Circle helps you restrict who in your family surfs what, and when. It also tallies how much time each person spends on any site. You might even want to monitor your own Facebook or Pinterest time (or maybe not…).

Circle also lets you put your whole home network on pause, sets up in about five minutes and works with your router.

Just $99 at MeetCircle.com may be all you need to win your family back from the web – at least for a few minutes a day.

Ransomware Adopting Self-Replication

Although some may have hoped that the threat of ransomware was on the decline, the reality is that it's quite the opposite. Until now, attacks seemed to be targeted directly at its victims, but Microsoft warns that may no longer be true. With their discovery of self-propagating ransomware it's vital to fully understand the possible risk of infection.

Ransomware, the malware that locks up infected systems and demands payment to return access to users, has been steadily increasing its infection rate over the course of this year. Enigma Software reported that, "After staying steady for the last six months of 2015, ransomware detection has begun to climb; February saw a 19 percent increase over January, while March had almost a 10 percent increase over February. Then, in April, infections more than doubled."

And as if that wasn't frightening enough, Microsoft announced last week that a recently detected ransomware software was found copying itself onto USB and network drives. The ransomware, titled ZCryptor, disguises itself as either an Adobe Flash installer or a Microsoft Office file to trick users into opening it.

Once opened, it displays a prompt that says "There is no disk in the drive. Please insert a disk into drive D:". If you see this after opening a suspicious file, it is most likely ZCryptor trying to distract you while it works in the background to add a registry key that buries itself deep in your system and begins to encrypt your files.

Although previous ransomware iterations like Alpha Ransomware had the ability to find and encrypt files on shared network drives, security experts believe this is the first time a ransomware variant has included self-replication via removable drives into its framework.

When it was first detected in May, Microsoft found ZCryptor singling out 88 different file types for encryption. However, later on a security expert analyzed the ransomware and found 121 targeted file types — inferring that creators of the malware were continuing to develop its source code.

It's commonplace for ransomware to demand payment to be made in Bitcoins as they're an almost totally untraceable online currency. ZCryptor is no different, demanding 1.2 Bitcoins (500 USD) unless payment is more than four days after infection — then it increases to five Bitcoins (2,700 USD).

Compared to other more complex security threats, ransomware is still relatively easy to avoid. Always verify the source of email attachments and website downloads before opening files, disable macros in Microsoft Office programs, maintain regular backups and update your security software.

Still concerned about security at your company? It doesn't have to be as difficult and draining as you may think. Contact us today at 701-364-2718 or info@imsnetworking.com for advice on keeping your network protected around the clock.

Bits & Bytes

Want to know your Lyft or Uber passenger rating?

Ratings are a two-way street with both Uber and Lyft. Of course, as a passenger you can rate your driver. Yet passengers are rated too, by their drivers. To find your average Uber passenger rating, open your Uber app and tap the menu bar in the top left corner. Then follow this path: Help > Account > "I'd like to know my rating." Tap "Submit" on the explanation page and your rating should then appear. Lyft has no such system, however their support team may send your average passenger score to you if you request it. Want to improve your score? Be nice to your driver and show up at your pickup location on time.
-Glitterless.com

Forget apps…here comes the voice-controlled future.

Soon, we won't be fumbling around with a gazillion different apps, trying to figure out which one turns off the sprinklers in the front yard… Apple Siri, Amazon Echo and now Google Home all point to the future of digital living. When it comes to voice plus smart machines vs. finger taps on a phone, voice wins, hands down. You don't want to use a weather app, you just want the forecast. Your customers won't go to your website and download an app; they'll interact with your business in some way by voice. That future will arrive in the next five to 10 years. Will your business be ready?
-Inc.com

Skip the airport – just hop in your e-jet and fly!

By 2018, owning your own battery-powered VTOL (Vertical Takeoff and Landing) two-seater could be one step closer to reality. That's the plan for the Lilium Jet, being developed in Germany under the auspices of the European Space Agency. This Jetsons-looking aircraft sports "fly-by-wire" joystick controls, retractable landing gear and gull-wing doors. Its developers claim it will have a top speed of 250 miles per hour and could be available to the public as soon as 2018. Designed for daytime recreational flying, it's quieter – and safer – than a helicopter, thanks to its battery-powered ducted fan motors and intelligent, computer-controlled takeoffs and landings. And pricing, according to its developers, will be far less than similar-sized aircraft.
-GizMag

Is your mobile website stressing people out?

Of course, page-load times can affect conversion and brand perception. But did you know they also affect user heart rate and stress levels? According to a 2016 study on mobility by Ericsson, page-loading delays lead to an average 38% jump in heart rate. Remember the last time you watched a horror movie? It's about that stressful… Not how you want your visitors to feel. To keep your page loads painless and your visitors happy, make sure your website is mobile-friendly. It needs to be quick and easy to navigate and engage with. You have a lot at stake in your website – and making it stress-free for visitors could make a big difference.
-HubSpot Blog