AITS Newsletter

AUGUST 2016

Ransomware – A Rising Threat [By Abraham John]

Simply put, ransomware is extortion and thievery by electronic means. Ransomware thieves use fear, intimidation and embarrassment to blackmail and extort payment from their victims.

Ransomware is malware (think of them as viruses – unwanted & uninvited "guests") that locks users out of their computer systems or data after which, the criminals send out threatening messages demanding payment.

The method of infections can be malware infected websites which will deliver their infectious payload when the site is visited or a message from a trusted source that entices you to open an attachment that contains the infectious payload.

The motive behind ransomware is quite pedestrian. It is about money. Other types of cybercrime may have political, personal, religious or moral agendas that drive the activists/criminals but ransomware offers an easy and relatively safe path to benefit from criminal activities.

According to a CNN news report, $209 million was spent by businesses and organizations to recover files locked by ransomware. The average payment ranges from $300 - $5000 for individuals and it is much higher for businesses and organizations. According to the Calgary Herald, the University of Calgary was attacked on May 28th, 2016 and paid $20,000 CDN (about $16,000 US) to obtain the keys to decrypt their files that were encrypted by ransomware. The LA Times reported on February 18, 2016 that Hollywood Presbyterian Medical Center paid $17000 as a result of ransomware. All payments take place via bitcoin which renders the path untraceable. More on Bitcoin in our next issue.

Did you know that optical media like DVD's, Blu-Ray and CD's store information in binary referred to as pits and lands?

A ransomware attack usually starts when an email from a trusted source that has a malicious payload is opened or via instant message (IM) or through social network channels like Facebook or a drive-by infection when visiting an infected or malicious site. The malicious malware delivers its payload which starts encrypting files it finds at all locations the user has visibility. This means that all Shared directories the user has access to could be impacted. This would also include OneDrive files. Since OneDrive uses a synchronization location within the user's space, any modifications made there are then synchronized to the cloud. The end result is that your files in the cloud would be modified with local infected copies. The encryption key has been, until now, an AES-256 randomly generated one-time key. From a practical standpoint, this is unbreakable.

There are 3 types of ransomware. The encryption variety or Crypto-ransomware encrypts user files, rendering them unusable and there is communication, either by a file or pop-up demanding payment. There may be a lock screen but there are many variations. Crypto-ransomware also may have a time limit, after which the files are permanently deleted.

The Lock screen ransomware locks the screen and demands payment but no files are encrypted.

The third variety is the Master Boot Record ransomware (MBR). This prevents the computer's operating system from booting up. A ransom demand is displayed and the machine is rendered unusable until this demand is met.

With the rise of Internet of Things (IoT) and home/facility/venue automation, variations of this type of threat can render not just a work or home PC useless, it could be your air-conditioning system or your refrigerator or it may even deny you entry to your home. You can easily imagine scenarios where "the bad element" starts to invade not only our electronic space but also our physical one.

The threat of ransomware is real and rising, so what can we do?

As users of technology we can take steps to protect ourselves and minimize the impact.

- Visit reputable sites and restrain yourself from visiting sites that appear questionable or suspicious. Look at the link by hovering over it with your mouse before clicking.
- Backup your files and check your backups periodically.
- Don't fall prey to phishing attacks. We have an article in this issue that provides you with some tools on how to guard yourself against phishing.
- Trust but verify. Was it actually your trusted friend who sent that that email or by a bot herder masquerading as your friend.
- Perform regular operating system and application updates.
- Use an up to date anti-virus program. As UNT employees you can download our antivirus software offering from https://itss.untsystem.edu/security/antivirus-download
- On Windows machines, use the "Show file extension" option
- Turn off the computer when you will be away from it for a reasonable period of time. A computer that is off can't be attacked.

Which of the following numbers is least like the others? (1, 3, 5, 7, 11, 13, 15)

As a home user if you do fall victim to ransomware, break your network connection immediately. The FBI recommends **not paying** the ransom. Try to recover from backups or by identifying the malware and researching tools that may help you recover. Contact residential IT support firms who may render assistance.

As an employee, if you fall victim to ransomware, break your network connection immediately and contact your direct IT support right away. We are here to help and get you operational in the most effective and efficient way possible for all events that take place at UNT or UNT owned hardware.

Malware/viruses, like their biological brethren evolve, with help from their masters, and variants show up with traits that we may not have seen. In this arena, vigilance is key and regardless of the tools and knowledge, any one of us could fall victim to this crime. No one is immune.

Let's work together to promote a safe computing environment!

Managing the influx of email [By Aaron Powers]

I think most of us will attest that we receive a lot of email these days, sometimes to the point that managing our mail feels like a fulltime job by itself. I've helped a lot of users and seen many approaches to handling the task (and many non-approaches too). For the users out there that don't have a system in place, here are a couple ideas and tools that might save you some sanity.

Create subfolders and route mail automatically

You can add folders within your Inbox to help organize mail by subject or sender (or anything that makes sense to you). I do this and then create Rules (right-click a mail item and choose Rules→Create Rule) to automatically place mail in those folders for review at my discretion. For example, if I get daily budget reports, which are probably important and need to be reviewed, I don't necessarily need those cluttering up my main view. I can route those to a folder and when I'm ready for that information, I know to find it. One email a day may not make much of a difference, but if you're routing 100 emails a day, it can really save you some time.

Use Flags and Reminders

There are many ways to keep track of items you've already dealt with, and here's my basic approach:

As I read through my mail items, I "Flag" them. When I finish reading the item, if it was purely informational and I won't need to interact with it again, I mark it as complete. Otherwise I leave it flagged, and if it has time sensitivity I right-click it and add a reminder that will ensure it gets addressed by an appropriate date. I add the Tasks pane to my view (View→To-Do Pane→Tasks) which allows me to quickly survey pending topics and plan accordingly.

Clean up!

One of my favorite features of the Outlook desktop client (for Windows) is the Clean Up function. If I right-click my Inbox, then choose "Clean Up Folder", it iterates through every mail item and gets rid of any duplicate/redundant data. If there is a back and forth chain of emails, for instance, it might delete all items except the last (IF AND ONLY IF the last email contains all of the information from the entire chain). If the thread breaks into sub-threads, it will make sure to only delete items that contain information found later on (including attachments). Because I use my main Inbox folder as the primary (email) workspace, it really pays to cut down on the clutter and I run the cleanup many times a day.

These are just a few ideas that may help some of you, but there are many more tools available to use and alternative approaches to take. Don't be afraid to reach out to us with questions or comments about email, applications, and especially about how we can better help you succeed with technology!

The very first email was sent sometime in late 1971 by Ray Tomlinson (April 23, 1941 – March 5, 2016) and he sent it to himself.

Phishing: Don't click that link! [by Jason McMullen]

Greetings. I hope everyone is having a great summer. A new academic year brings new attempts from the bad guys of this world to get their hands on passwords, personal information, and your money!

What is Phishing and how does it work?

Simply put, phishing is an attempt to trick individuals into providing personal or financial information to criminals. Phishing is usually attempted via email, but can just as easily arrive as an instant message, social media communication, or text message. On the surface, phishing messages appear to come from legitimate sources like a bank or IT support. These messages will instruct a user take some action like clicking on a link, logging onto a fraudulent webpage, or providing other personal information such as credit card numbers. Phishing relies on confusing the targets of the scam to coerce them into providing this information.

What do phishing attempts look like?

Phishing can appear authentic and will often use company logos or address a user by name. Sometimes these messages claim that a user's account has become suspended or that it will be deleted if they do not respond. Other messages might claim that the user has already become a victim of a hacking scheme and they should login or provide their credentials to protect themselves. Methods used by phishers become more and more sophisticated as we become more informed regarding their tactics.

How to protect yourself!

Here is the simplest counter to phishing: Don't open suspicious email or click any links from a suspicious message. Remember that personal information or passwords will **never be requested** by financial companies, social network companies, or UNT IT staff. If you are unsure of the validity of a message, contact the agency directly through your normal means. For example, if you received a message from your bank that seems suspicious, call or email them directly to inquire about the message. Do not click any links or login to any websites that you are directed to within the email. While at UNT, forward any suspicious messages to your local IT support. We can investigate and can take action to block these messages in the future.

The first computer virus was released in January 1986 and it was called Brain. It infected the boot sector or media formatted with the DOS file allocation table (FAT) system. It was written by two brothers from Pakistan.

Oops. I clicked the link and entered my account information. What now?

Don't panic! Do the following and everything will be fine:

- ***Contact your local IT support at UNT:*** Your local IT department can help identify what campus resources might be affected. We are here to help!
- ***Login directly to any accounts that either may have been affected or share the same username or password:*** Do this from another computer or phone if possible. Follow the instructions on those sites to change your password. (TIP: it is a good idea to keep your usernames and/or passwords different for different sites. This limits the amount of reach that a bad guy would have into your accounts.)
- ***Contact your bank, credit card companies, and other financial institutions:*** If you entered login information for your bank or provided personal information to an unknown source, contact these folks right away.
- ***Scan your computer for malware:*** UNT ITSS offers free downloads of McAfee virus scanning software to all UNT employees. This software can be found at https://itss.untsystem.edu/security/antivirus-download.

Excel 2016 for Mac Offers Genuine Business Functionality [by Chris Johnson]

A familiar trope in IT circles relates the traditional view that while Apple products may look nicer, Windows machines are required for actually "getting work done." Perhaps ironically, one company that is challenging that notion is none other than the maker of Windows – Microsoft.

With its latest release of the workplace-standard Office suite of applications, Office 2016 for Mac, Microsoft brings a number of features to the Mac OS X platform that had been sorely lacking from previous "for Mac" versions. Dave Coursey provides an excellent discussion on how this move reflects Microsoft's strategy for the so-called "post-PC" world here. Microsoft Excel has received a major functional overhaul and is the beneficiary of a number of improvements that data analysts and other number crunchers will appreciate. One such feature that is new to the Mac OS platform in this release is the Analysis ToolPak plugin which features support for a number of analytic functions, including ANOVA and Regression tests. (NOTE: The Analysis ToolPak is installed but not enabled by default – for instructions on how to activate the plugin, Microsoft has provided instructions here.) Microsoft has also included a number of popular Formulas that had been missing in previous Mac versions of Excel. Power users of Windows-based Excel will be pleasantly surprised at the number of keyboard shortcuts that Microsoft has ported to the Mac, as well (here's a handy reference from Microsoft).

With its latest release, Microsoft seems genuinely committed to providing all Office users with the full functionality of its industry-leading product suite, independent of a specific OS platform. While mobile app-based versions of Office aren't quite up to speed with their desktop/laptop counterparts, and even though we may never get an Office version for Linux (despite what Jack Wallen says), Office 2016 for Mac goes a long way toward making Apple products a legitimate alternative for business users interested in "getting work done."

VisiCalc, the first spreadsheet program and one that was made for the Apple II was soon eclipsed by Lotus 1-2-3 as the preeminent spreadsheet program for the PC. It was written in x86 Assembly and the original one was written by programmer Jonathan Sachs.

Received an odd Facebook friend request? Knowing these 3 tips can protect your identity…

[by Troy Bacon]

Have you ever received a Facebook friend request, but couldn't remember if you knew that person? You begin to think… Is this a distant relative? An old friend from high school? An acquaintance I met a few weeks ago at a business function?

It can be difficult to remember the names and faces of all the people we meet. Hackers know this, and they are starting to target us on Facebook.

If you receive a Facebook friend request from someone you don't know, it could be a hacker trying to steal your personal information on Facebook. Most users on Facebook have their personal information available to their friends, so if a hacker can become your friend, they see all of your information, including your birthdate, phone number, and email address. If you have defined relationships in Facebook, then they can see the names of your family members.

If you want to protect your identity, follow these easy steps the next time you receive a friend request…

1. **Scan your friend request**. Don't automatically accept a request, but check the other person's profile to see if it looks legitimate.
2. **Check for spelling errors or poor grammar**. Many of these hackers are from overseas and they don't have a good understanding of the English language.
3. **Check to see if you have any mutual friends**. If you have mutual friends, then chances are good that the person is not a hacker.

Did you know that scientists have successfully written a paragraph 1016 bytes long – almost a KB – in binary digits that are 8 bits in length using atoms? They took their inspiration from Richard Feynman who envisioned that one day atoms could be arranged to store information. No surprise, this was done in binary with each character being composed of 8 bits or a byte.

Did you know that Sir Timothy John Berners-Lee is known as the inventor of the World Wide Web and he executed the first successful http communication between a client and server in 1989?

HIPAA at UNT [by Chris Stoermer]

Who really understands HIPAA? Do you even know what the acronyms mean, or to what individuals, organizations and data sets it actually applies?

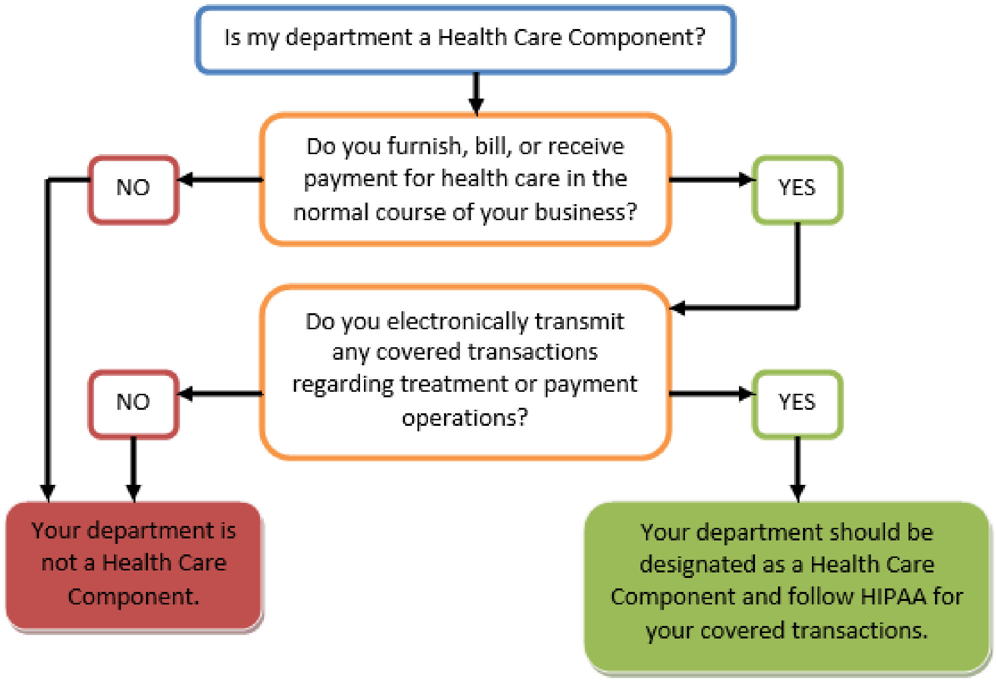
HIPAA stands for the Health Insurance Portability and Accountability Act of 1996 which regulates the use and disclosure of Protected Health Information held by "Covered Entities". Notice that punctuation mark after "Covered Entities". That is a period. In English, that mark is used to express the finality of a statement, meaning nothing comes after this mark. The reason for laboring over this point is that if you and/or your organization do not meet the definition of a "Covered Entity", you are not regulated by HIPAA…PERIOD.

So, what is a "Covered Entity"? Simply put, Covered Entities are Health Care Providers who transmit any health information electronically in connection with certain transactions (like your doctor), Health Plans (Insurance Companies, etc) and Health Care Clearinghouses (companies that process Health Insurance, etc).

It is important to note that not all Health Care Providers are covered. Only those that transmit protected health information electronically in connection with a covered transaction are regulated by HIPAA. For example, a plastic surgeon who only deals with direct payment from his customers and does not file any covered transactions for insurance may not be a Covered Entity.

UNT recognizes that some parts of the university are likely to transact HIPAA regulated data, so it has self-designated as a Hybrid Entity. Hybrid Entities have both regulated and non-regulated activities. While the institution as a whole is responsible for compliance, only the Health Care Components must follow HIPAA.

How do you know if your area should be designated as a Health Care Component?


Is my department a Health Care Component?
Do you furnish, bill, or receive payment for health care in the normal course of your business?
NO
YES
Do you electronically transmit any covered transactions regarding treatment or payment operations?
NO
YES
Your department is not a Health Care Component.
Your department should be designated as a Health Care Component and follow HIPAA for your covered transactions.

20 Years of Pressing Start [by Christopher Horiates]

The year was 1995. The company eBay was founded. The DVD for disc computer storage is announced. The world population was at 5.6 billion. A little button with the word Start became a part of our lives. In 1995, Microsoft introduced a little button on the bottom left of a computer screen that changed the world forever. This of course is the Start button and Windows 95. Remember the TV commercial with the Rolling Stones "Start Me Up?" See if you can't stop humming that song for the rest of the day ☺

Yes, it's been 20 years since the world first saw the Start button in Windows 95. It's been 30 years since Windows 1.0 was released. Where has the time gone? It was a new way to compute. At the time it really put the Graphical User Interface (GUI) into the forefront. It made getting to programs easier, gave file and program structure a purpose. The Start button was the start of a computing revolution that has only gone up from where it started, no pun intended. It became such a part of our lives that when Windows 8 came out the world revolted that the beloved Start button, while there just used differently, had gone away. Microsoft heard the cries for the Start button to be brought back and in Windows 10 it has made an appearance, as a new hybrid. We now have Live Tiles that provide information without clicking on the program. The familiar folder structure is back. Using Windows for those who have for the past 20 years, while it cosmetically looks different, starts with a click on the bottom left of your screen once again.

Like it or love it Windows has changed the world. It still has the largest market share of any desktops OS and Windows 10 is being adopted at a very fast pace. We are able to search for answers to just about any question we can think of, perhaps get a right answer, and consume more information in days then those before us could in a lifetime.

Enjoy what the future holds and happy and safe computing!

Microsoft Windows NT, the ancestor or the current Windows server/desktop OS's has a checkered past. For history buffs and conspiracy theorists OS/2 and Windows NT both saw their respective inceptions at Microsoft and arguments rage as to the how Windows NT was created. OS/2 was written for IBM and Windows NT was sold as a Microsoft product. Windows NT was a 32 bit OS. Windows NT and Windows 2000 incorporated an OS/2 subsystem. However Microsoft abandoned OS/2 in 1990 and concentrated completely on Windows.