AITS Newsletter

December 2016

Table of Contents

Prototype resonant cavity thruster built at NASA Eagleworks, 2014

Will this give us propellant less propulsion system?

Administrative Information Technology Services and you: How can we help Administration? [By Aaron Powers]

Information technology is always growing, and the way IT services are provided at our university has, of course, changed as well. When directly helping people we support, which is administration, I often hear "I'm not sure if this is something you do, but…", and for good reason; information technology is an incredibly wide field and it takes many teams here at UNT, and in the world, to make it all work together.

So what exactly does AITS do? Well, we provide services including file, application, printer, network, web, account, camera, security, POS (point of sale), desktop support, reporting, A/V…and more! However, the **MOST** important thing we do, is keep up with the ever changing landscapes of technology, UNT organization, and business trends. This allows us to **serve as your single point of contact for ALL of your technology requirements.** In other words, you don't need to know exactly what we do! Just know that we can either help you directly, or we can work on your behalf with the people most appropriate. All you need to know, is what you want to do with technology, and maybe not even that! We're happy to look over business processes with you and recommend ways in which technology can help improve your operations. As you consider external contracts for technology, whether they be hardware devices or services, we can help act as liaisons and as a help in navigating the technology landscape put forward by external organizations. This will have a very direct effect on your bottom line in getting goods and services you need at the right price. We already do much consultation on campus, and there's a chance another area is using something that might be useful to you too. Pooling these types of efforts can often mean better licensing costs, which helps everybody too.

As the individual areas of technology expand, and more specialized knowledge of particular concepts is required in each area, the number of different parties involved will rise and this single-point-of-contact approach will become more and more valuable for you. Please know that you are encouraged to lean on us now, and in the future. We are your technology team and we are here for you!

If "through" and "threw" are pronounced the same, cross out all of the even numbers in the line below. If they are not, cross out all of the odd numbers. If Tbilisi is the capital of Georgia, add all of the numbers that are left. If it is not, multiply all of the numbers left. Your answer?

1 2 3 1 2 3 1 2 3 1 2 3

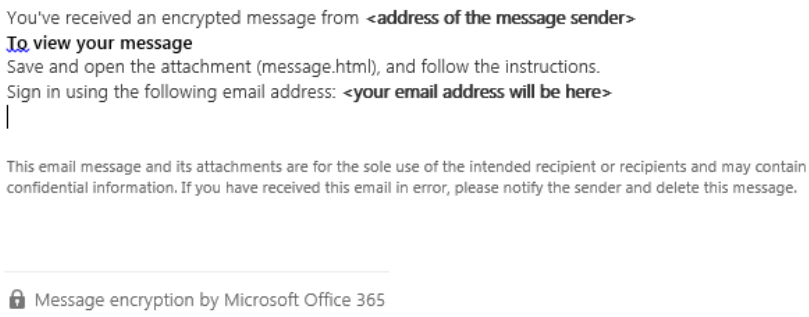
Sending Encrypted Email Messages [By Abraham John]

Did you know that you can send an encrypted email to someone within UNT or to an external email address from within Microsoft Outlook? Well, you can! Let's take a brief journey on how this is accomplished. I'll provide a few steps on how this can be done and also include an excellent video that Mr. Jason Gutierrez, messaging team lead, has created. Between the two approaches learning this may, hopefully, be a painless and enjoyable exercise.

The process of sending an encrypted email to someone within UNT or to an external email is the same. To send an encrypted email:

- Enter the email address of the recipient
- Start your subject line with "#Secure" - without the quotes
- Type your message as normal, attach documents as you normally would
- Click Send
- That's it!

Reading an encrypted email just has a few more steps as a result of the added email security. When you receive an encrypted email that has been sent from Outlook, you'll see a message body that looks like the one below and you'll also have an attachment named "message.html".


You've received an encrypted message from **<address of the message sender>**
To view your message
Save and open the attachment (message.html), and follow the instructions.
Sign in using the following email address: **<your email address will be here>**

This email message and its attachments are for the sole use of the intended recipient or recipients and may contain confidential information. If you have received this email in error, please notify the sender and delete this message.

Message encryption by Microsoft Office 365

When you save/open the "message.html" attachment you'll be taken to a page that provides some basic information about the sender and recipient. There is additional instruction that prompts you to sign in if you will be using your work or school account or to use a one-time passcode in the case of external entities who may not have an account on Office 365. If you select sign in, you'll see another page that lets you choose "Microsoft Account" or "Work or school account". **For our purposes, choose "Work or school account".** You'll be presented with a dialog box where you can enter your full work email address and associated password. Once that is verified, you'll be taken to your encrypted email.

At this point you can read, reply, print or forward – normal activities but you can't delete from this location. Once you are done, there is a "Sign Out" option at the top right of the Encrypted Message screen header bar. Click that to sign out.

If you click on the one-time passcode, Office 365 will send you a regular email with a one-time passcode. Go to **your email client to see what the passcode is** and either type or paste it into the passcode text box in the Encrypted Message window. If the computer you are using is not a public machine, then you can select the private computer check box so that the passcode is remembered for 12 hours and you don't have to reenter the passcode if you happen to reopen the encrypted message. Click on Continue. You encrypted message is opened and you can do normal things like read,

December 1, 1862 – President Abraham Lincoln gave the State of the Union address to the 37th congress.

Did you know that the 2.4GHz Wi-Fi signal travels better than the 5GHz Wi-Fi signal through walls and windows? This might be handy if you are trying to connect to your access point at home from a different room than your Wi-Fi router.

reply, print or forward – but you can't delete from this location.

Given how easy it is to send an encrypted message and since you are not restricted to just recipients within UNT, this should be the standard means by which sensitive materials are communicated within UNT and to colleagues outside UNT.

While this is a powerful tool, not every email should be subjected to mechanism. It does add a few steps on the recipients' side and any replies coming back to you will add the same number of steps on your side. Encrypting non-sensitive messages may prove frustrating on the recipient's side.

To quote Spiderman "with great power comes great responsibility" ☺, you have the power, so now it is your responsibility to use it wisely, productively and in keeping with the nature of the data/information being communicated.

The video that Mr. Gutierrez has created can be found at this link: https://myunt.sharepoint.com/portals/hub/_layouts/15/PointPublishing.aspx?app=video&p=p&chid=3060c23c-0449-4055-bc38-2a9157c97d9e&vid=22892c9d-96fa-413d-bfa1-ecfdf36a85c0&from=2

You'll have to sign in with your work email and associated password when you click on the link above.

As always, we at AITS, are here to help and provide any and all assistance with all your technology needs.

For those among the readership who enjoy the major English Romantic poets – here are a couple of suggestions from Percy Bysshe Shelley – Ozymandias and Loves Philosophy – enjoy ☺

Pop-up Blockers [By Chris Stoermer]

Ever been surfing the web, doing research on the latest hot topic like the Brangelina breakup, and when you click one of the search hits more than one window loads, none of which seems to be related to your search topic? Even worse, have you ever clicked on a web link only to get a blank page and, no matter how many times you refresh, nothing appears? Chances are, when you explained this behavior to your IT support person, you were told to add an exception to, or turn on/off, pop-up blockers…..I am sure your next thought was, "What the heck IS a pop-up and how do I know if I should be accepting, or blocking it?"

To understand pop-up blockers and why they are both useful and a nuisance, we need to understand what they block: pop-up windows. Pop-ups originated in the 1990s on Tripod.com when a resourceful web coder named Ethan Zuckerman wrote web code to change the way his company published web advertisements. Before this time, ads were coded into web pages which triggered many consumer complains due to the extended page load time for the advertisements. Zuckerman's code allowed advertisements to be launched in separate window from the main content. Pop-ups also allow the parent page to redirect the internet consumer to new content without disrupting the existing page content. Unfortunately, this code was quickly modified to create 'ad storms' and was heavily abused on many early commercial web sites. These ad storms routinely would crash machines due to the number of windows that would open.

The solution to control these ad storms was to integrate the pop-up blocker feature into the web browser. This feature looks for the code pattern of the pop-up and blocks it.

Great! Problem solved.

No more pop-ups, right? Well, not exactly.

There are still many good reasons for programmers to use the pop-up window code and many web servers still rely on pop-ups to take care of presenting data to the consumer. Pop-ups also can be used to pass a consumer from one system to another. For example, when we log into the myUNT portal and click an EIS link, a new window, or Window Tab, opens and you get into EIS without needing to put in your username and password again.

Pop-up Blocker settings are similar in every browser, but different enough that you will want to do a quick Internet search to find out how to manage your browser's settings. Just search for "manage pop up blocker" and add on your browser's name.

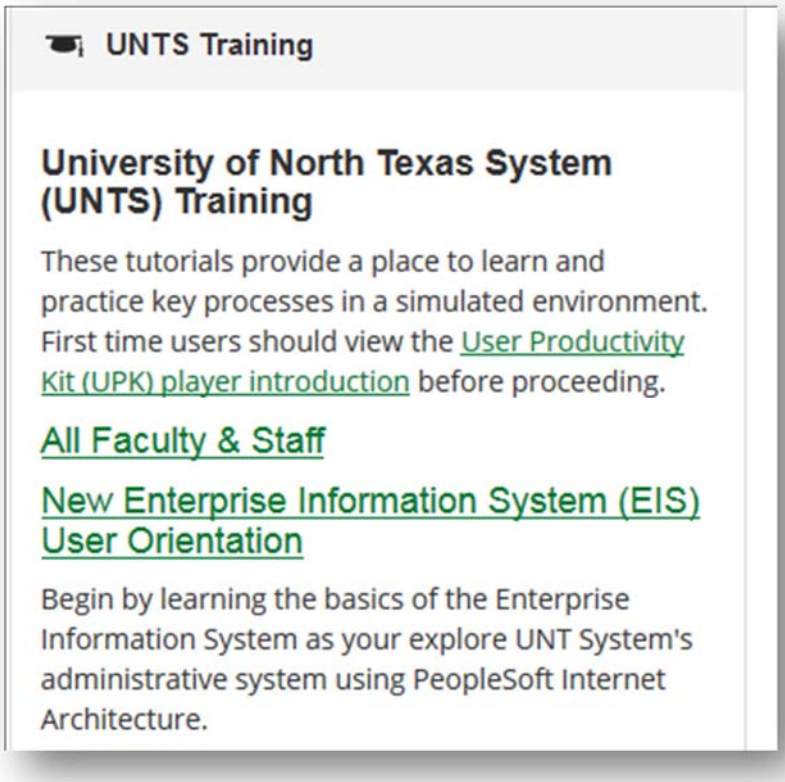
Author's Internet Safety Alert: The current internet safety recommendation is to leave pop-up blocker settings enabled and only add exceptions for systems you trust and know need to be allowed to show you pop-up windows.

For the readership that may enjoy D.H. Lawrence – try the short one on "Self-Pity". ☺

Tutorial: New Enterprise Information System, EIS, User Orientation [By Dorothy Flores]

Are you new to EIS? Do you know what it is and how to use it? Have you looked for or wondered where to find available training? If you are new to EIS, there is a training tutorial available just for you. It's called "New Enterprise Information System (EIS) User Orientation."

You can find this training in several places, but the best option is within the my.unt.edu portal. Once logged in, go to the Human Resources tab. Scroll down until you see a box displayed on the right side, entitled "UNTS Training." In there, you will find links to several training offerings, along with the new user training tutorial, which will look like this.



Included in the New EIS User Orientation is an EIS Overview, information about security access and how that works, basic navigation features, and how to search for and retrieve data on a page in EIS. All of these are core concepts that any new EIS users would benefit from knowing, as they build a foundation of knowledge about using EIS.

All training in this section is provided within a tool called User Productivity Kit (UPK), which allows the user the ability to click through the information, in a "Try It" mode to see how the functionality works. There are also instructions in each training offering which shows you how to use the UPK tool.

Check out other available EIS training, like Employee and Manager Self-service, EIS Finance Query Basics, and EIS Time and Labor for UNT.

For you sports fans, December 1, 1963 – first shutout by the NY Jets against the Chiefs!

Phishing [By Paula Mears]

The internet has become a central component in our everyday lives and because of this, we are targeted over the web frequently. With the use of email as major form of communication, intruders attempt to infiltrate our inboxes with illegitimate messages with schemes ranging from selling products to us, to stealing information from us. With this being said, there are many differences between plain old spam and the ever increasing tide of phish scams.

Phishing attempts can be dangerous and most of them are quite convincing. They often appear as emails or messages from authentic companies requesting that you send personal information to them for what may seem to be a legitimate reason. If you fall for it and input your information, these scammers can now use this information to steal from you.

Spam emails are a little less invasive. Spammers will harvest email addresses from various sources such as websites, forums, and social media websites then send pointless email or "junk mail" to you. There is little you can do to prevent spammers from getting hold of your email address.

What is Phishing?

Phishing is a form of fraud in which the attacker, posing as a trusted source, urgently requests employees to disclose personal and confidential information like account information, log-in IDs, or even passwords. Phishing email tries to trick you into giving up your personal information, such as login id, password or credit card number. Phishing messages usually have a threatening tone in an attempt to fool you into thinking there will be a consequence if you don't respond.

What is Spam?

Spam is a form of commercial advertising which can typically be seen as a mass email. Spam email is a cost-effective medium used to reach a large number of people with the purpose of getting some sort of response. Span or junk mail, is unsolicited email that tries to sell you the "latest and greatest" product or service. Spammers send their messages to hundreds, thousands, or even millions of email addresses at once and don't attempt to acquire sensitive information.

The UNT System Information Security team is encouraging employees (as always) to submit any recent phishing emails to the security team email box at security@untsystem.edu. Please submit (forward) any phishing email received to our information security inbox as an attachment at **security@untsystem.edu**

How to Forward an Email as an Attachment [OUTLOOK]

1. On the Microsoft Outlook main page, select the Email you want to forward as an attachment.
2. Click on the Home tab.
3. Choose More from the Respond subcategory; click on Forward as Attachment.
4. Fill out your desired recipient(s) and the subject/body of your email; click Send.

Personally Identifiable Information (PII) [By Mickie Tate]

What's the big deal about PII – and what is it anyway?

What is PII? PII is Personally Identifiable Information. This constitutes a number of different types and combinations of information that could be used to singularly identify an individual by using information which could not have been obtained from public means, and there really isn't a one stop shop for defining what PII is.

Some of the items that can make up PII:

HIPAA – Protected Health Information (PHI)
Payment Card Industry (PCI) - Credit Card Information
Passport information
Driver's license number
Social Security number
First or last name (if not common)
Date of birth
Country, state or city of residence
Age
Telephone numbers
Email addresses
Gender
Race
Criminal record

The Health Information Technology for Economic and Clinical Health (HITECH) Act, which became effective on February 18, 2009 has quite a few revised sections as it relates to penalties. This should be viewed in conjunction with the Joint Guidance document on the Application of FERPA and HIPAA to Student Health Records

The key is being able to merge pieces of information together to personally identify someone.

Security of data is everyone's responsibility: from the CIO and CISO to the data managers and data custodians to the individuals who interact with the data on a daily basis. One way to look at it is would you want your driver license, credit card number, personal banking or passport information put where it could be exposed to anyone in the world? That is what happens when we store, transmit or handle other people's sensitive information in an unsecure manner, we expose others' information to potential compromise.

From the UNT's perspective, a compromise of PII could result in damage to the university's reputation, a loss of public trust and potentially fines, penalties or lawsuits. From the personal perspective, a compromise of PII could result in public embarrassment, targeting, locating family members or even stalking.

Securing information doesn't stop with safeguarding the electronic system(s) on which it resides. Paper copy information should never be left unattended on printers, or in office areas and should always be locked away when not being used. And when destroying sensitive paper copy information, it should be cross cut shredded, as ribbon cut shredding can be ineffective. Never just discard it in a waste basket. Also, never send PII in an unencrypted email. If you do have to send encrypted PII, always have your supervisor's permission and the approved process to encrypt the email properly.

When in doubt, reach out to your AITS representative, the CISO, or the senior director of IT audit. One of these individuals gladly will be able to get an answer for you.

Let's all do our part in keeping UNT information secure.

Links to sites containing PII definitions and discussion:

UNT System Information Security Handbook - https://itss.untsystem.edu/sites/default/files/unt_system_information_security_handbook_2016.pdf

Handbook for Safeguarding Sensitive Personally Identifiable Information US Department of Homeland Security - https://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf

NIST 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

Did you know that most modern VPN processes encrypt your communication so that as it traverses the internet to get to your office, the contents are not visible until it is decrypted by the VPN gateway at the office?

7R\$76&LHQV Do you need to access UNT resources from off campus? [ByTroy Bacon]

If RXQHHGWRDFFHW817RQOLQHUHVRXUHV7IURPRIIFDPSXV, then you will need to connect to the UNT campus virtual private network931. It allows your off-campus computer to be on the UNT network in a secure manner. When using a VPN, all network traffic is encrypted through a tunnel, which prevents hackers from seeing the data.

If you are using a UNT-owned laptop computer, then the Cisco AnyConnect VPN already may be installed. Look on your desktop or in your Start menu for “Cisco AnyConnect”. If you see this item, go ahead and run the program. You will be prompted to enter your username, EUID, and password. You will then be connected to the UNT campus VPN.

If you are using a UNT-owned laptop computer, and you cannot find the Cisco AnyConnect client, then please contact our AITS Helpdesk at **940-565-4790**, and we will schedule a time to install it on your computer.

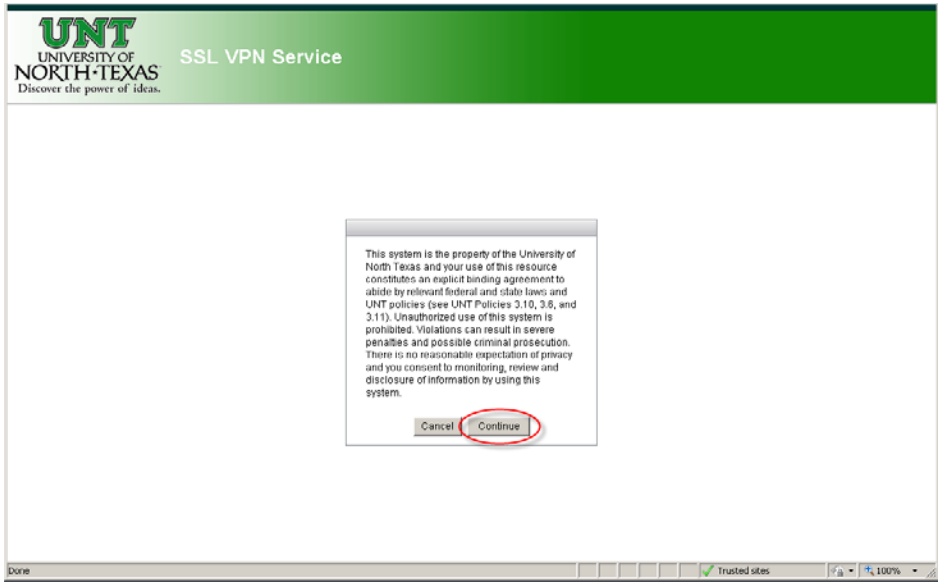
If you need to install the VPN client on a personal PC, then you will need to follow the instructions below. If you have any questions about the installation process, please contact our Helpdesk at the phone number above. While we cannot directly support personal computing devices, we can answer questions and provide guidance.

Installing the Cisco AnyConnect VPN Client

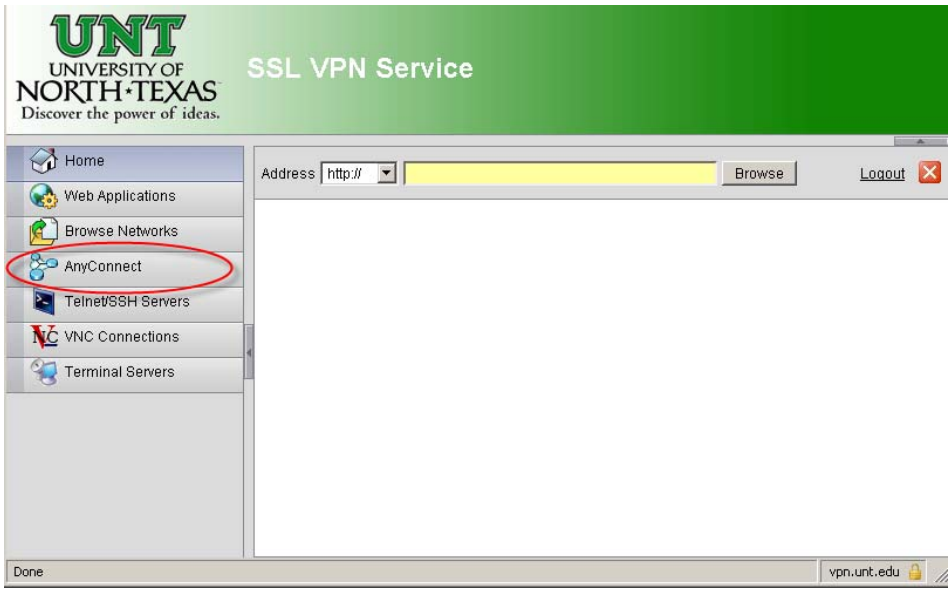
1. Open a web browser and navigate to: KWWSYSQXQWHGX.

   You will be presented with the following login screen.

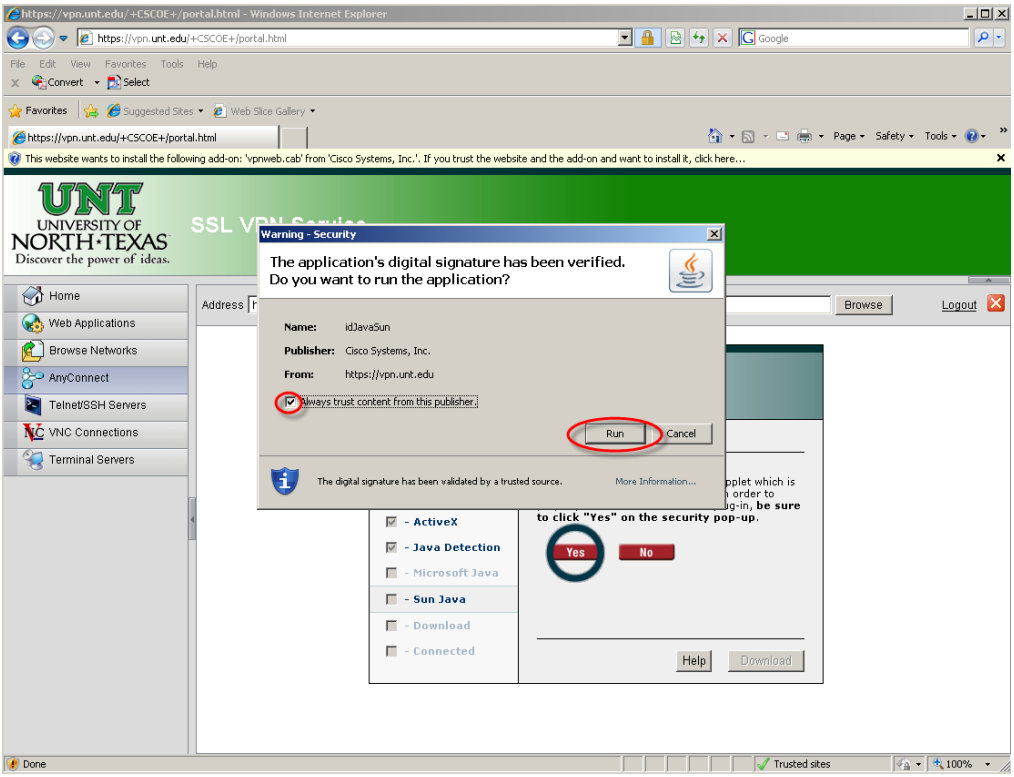
2. Leave the Group selection set to “General.”
3. Login with your UNT EUID and password.
4. Acknowledge the UNT Security screen by clicking “Continue.”



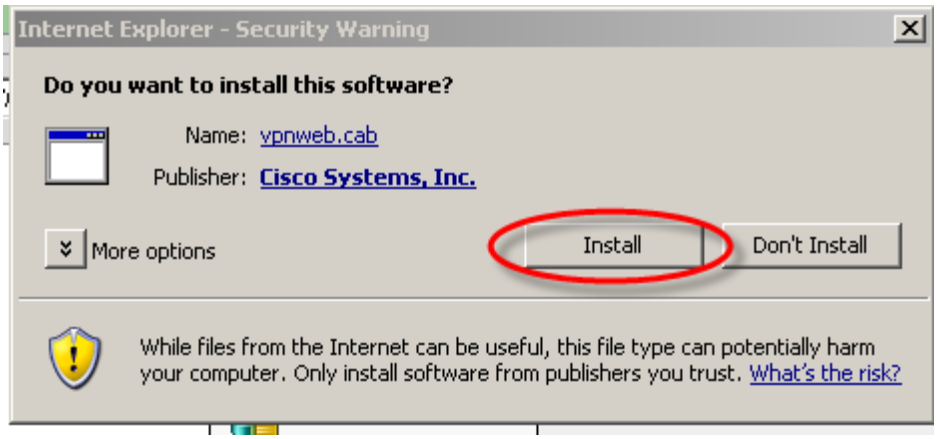
5. Select “AnyConnect”.

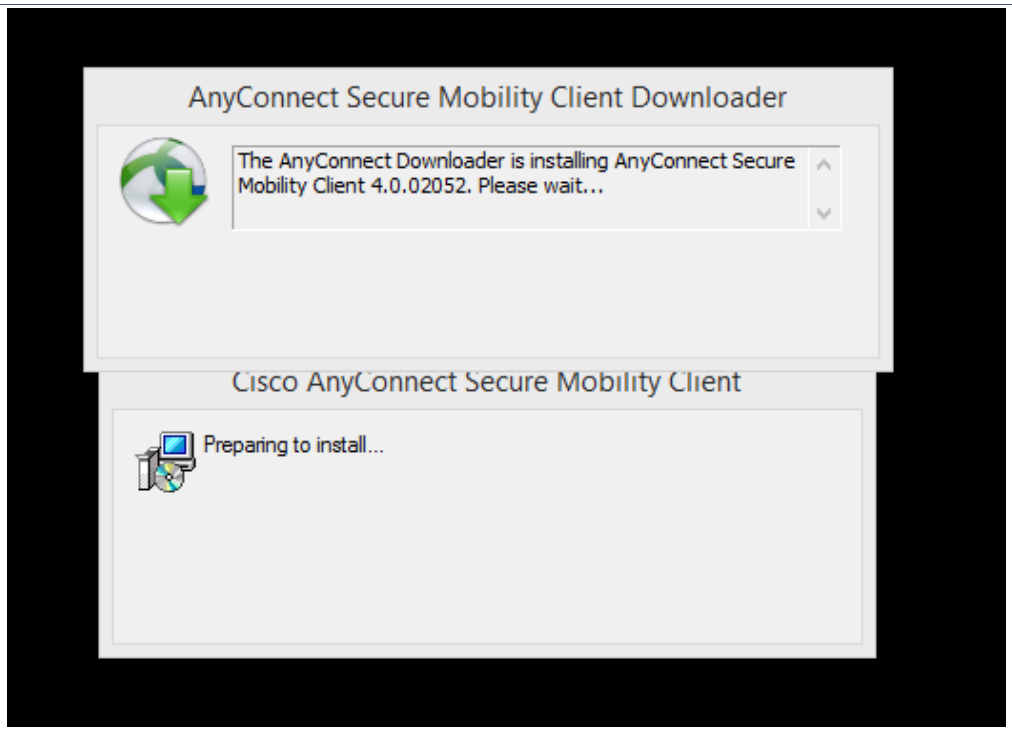


6. The first time you select this on your computer, you may be prompted to install some Active-X controls. Go ahead and allow these to be installed.

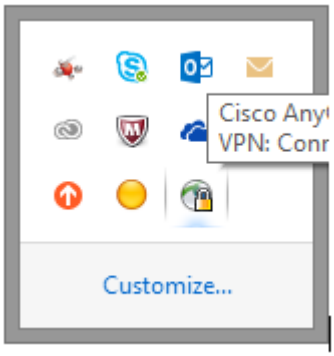


Click here, then select these two options.





7. At this point, the VPN client should be installed, and you will be connected to the UNT VPN. You can check the status of the VPN connection by hovering your mouse pointer over the Cisco AnyConnect button on the right-side of your task bar.



8. Lastly, you can toggle your connection to UNT by going to your task bar and right-clicking the Cisco AnyConnect button and selecting Connect or Disconnect. Please disconnect from the UNT VPN when you are not accessing UNT resources.
   If you have any questions or concerns, please contact the AITS Helpdesk at 940-565-4790.

Did you know that AITS now has a staff member, Joshua Avery, at our Frisco location? Talk to us about your support needs at Frisco.

A Beginner's Guide to EMV and Credit Card Security [By Jason McMullen]

Greetings! In an ongoing effort to reduce fraud and protect consumers and businesses, three major credit card entities, **E**uropay, **M**asterCard, and **V**isa, came together to standardize a new technology: EMV. Cleverly, they chose to use their initials to name the biggest change to the credit card industry in decades.

Simply put, an EMV credit or debit card is a specially designed card with a small silver microprocessor chip embedded on its surface. These cards are designed to be inserted into a card reader rather than swiped. Information encoded on the EMV chip provides an additional barrier against counterfeiting.

While Europe was quick to adapt to the change, it has taken EMV 20 years to become commonplace in the United States.

EMV cards were originally read much more slowly than the traditional magnetic stripe cards. However, the transaction times have been improving and that should lead to more companies adopting the technology in the near future.

Why EMV and Why Now?

Most readers of this article have EMV chip cards that have replaced their regular credit/debit cards. However, not all payment locations currently read chip authentication. By the end of 2017, all card readers will need to read chip cards or the companies themselves will be responsible for any fraud that would have been prevented by a chip.

How Does EMV Help? What Are the Limits of EMV

The Good

EMV helps in two primary ways.

1. The chip stores an authentication key that proves that the card is valid.
2. The chip also provides a one-time transaction number each time it is used. This transaction number prevents a criminal from obtaining a card number in a breach, for example, and printing a fraudulent card.

The Not-So-Good

New EMV cards issued to customers in the United States are chip-and-signature cards versus chip-and-PIN cards. With the signature option, criminals are already searching for weaknesses in the transaction number scheme. If/when this is cracked, fraud could still happen because signatures are not typically verified. Once a personal identification number, PIN, is required, a criminal would need to know the transaction number scheme and your PIN.

EMV does not offer any protection when using the card to make online purchases or through a mobile application. Because of this, industry-trend watchers expect online fraud to rise as it becomes more difficult to defraud brick-and-mortar locations.

What's Better? What's Next?

Unfortunately for us, EMV is not a true security technology. It is instead an anti-fraud and authentication technology. Chip cards still carry the unencrypted primary account number, PAN. And EMV doesn't protect credit card data that is stored on remote servers.

There are two additional technologies that will further protect banks and consumers from cybercriminals: tokenization and encryption.

Tokens replace the actual PANs with a substitute value that is unique to that transaction – unlike EMV that uses a unique number solely for authorization. The actual PANs are stored securely elsewhere and if the tokens are stolen during a breach, they can't be used.

Encryption scrambles the card information in a way that can only be decrypted with a key. Encryption happens at the moment the card is read and is not decrypted until it is processed. This prevents the PAN from being intercepted in transit over the Internet.

So what is best? The best is all of the above! As is usually the case, IT security is most effective when stacked in layers.

Happy shopping, everyone!

Internet of Things, IoT [By Christopher Horiates]

Is your refrigerator running? Why, yes.

Well, you better go catch it.

That is a joke we may all have heard at some point in our lives. Ask someone that question now and the answer you get might be let me get on my smartphone and check and while I'm at it I will you know what's in my fridge and oh by the way I just got my weekly grocery list sent to me from my refrigerator and the order has already been placed and the delivery time is later tonight.

Did you know that at higher frequencies, objects and walls appear thicker as a percentage of the wavelength? See comparison of 2.4GHz vs. 5GHz earlier in the article.

What just happened? A simple childhood joke has turned into your refrigerator ordering groceries for you?

Yes, that is the world we live in and will be living in in the not too distant future. We are more connected than ever and items you never once thought were able to get online now are able too. For better or worse the Internet of Things, IoT, is here and not going anywhere anytime soon. You most likely have heard of the term smart home, smart building, smart TV, smart car or smart – insert obligatory item. Everything that can be connected seems to be connected. While this may make our lives better, the dark side of IoT is what no one wants to talk about.

You may have heard about the massive internet outage in the news a few weeks ago. Did you look into how this happened or what caused it? Your Twitter feed or Netflix might have been interrupted, but did you ask yourself how did this happen? You might have been a part of the attack and did not know it. An army of "Smart IoT Devices" were all programmed to attack the servers in a coordinated effort to cause the outage. This is the first time something like this has occurred, that people know of. Basically, malware took over people's "Smart IoT Devices" in homes, business and such, and when the time came, it flooded the servers on the internet and took sites offline.

Could it have been avoided? Training for users and responsibility on the manufacturer to keep their IoT devices safe is important.

1. If you happen to have some IoT device in your home did you change the default password when setting it up?
2. Did you lock down your firewall/router to protect others from getting into it?
3. What about your Wi-Fi network? Is it the default SSID and Password to get on and default administrative password to log into the router?

Asking those questions – and knowing the answers – are two very simple things you can do to protect yourself and your family. Ever thought who else might be watching your kid sleep at night on that new Wi-Fi enabled baby video monitor? What about your car, did you update to the latest software to avoid that known exploit where someone can take it over? While these may all seem like doomsday scenarios, that fact is it's true and have happened.

On the manufacturer side the issue with them is they make so many of the IoT devices, phase them out quickly and do not bother to add basic security or update the firmware to fix known and exploited security issues. There are talks that just like other areas of technologies some standards be set and the wild west of IoT will be more controlled. Ideally automatic updates of firmware or better notifications of how and where to get them would be a good start.

Am I in favor of IoT and what it can do? Yes, of course. I like the idea of being connected, but I don't think we all fully understand the risk that comes with it. The pros and cons need to be looked at and considered when connecting things.

So, while checking in on your IoT device from your smart phone from anywhere in the world might seem like an improvement to your life, just remember the this rule: anything you don't want the rest of the world to see, know or access, don't put it on the internet.

Apple's New Approach to Privacy in iOS 10 [By Christopher Johnson]

With iOS 10, released in June 2016, Apple introduced several important changes in its data collection practices that have caused some alarm among privacy advocates. While the Cupertino-based tech giant has significantly expanded the amount of user-related data it collects and shares with app developers, it has introduced a sophisticated new method for handling that data, and claims the new measures ensure the collected data will remain anonymous.

Apple has started collecting more information about users…

Apple was founded by Steve Jobs, Steve Wozniak and Ronald Wayne on April 1, 1976. Ronald Wayne backed out 12 days later – Apple history lore!

In previous versions of iOS, built-in Apple programs (such as the Spotlight search app) gathered usage data from other installed apps installed on a user's i-device. Data would then be used to tailor a user's experience to their own unique preferences. The results include more accurately targeted search results in Spotlight and more desirable recommendations in the iTunes and App stores. Through iOS 9, this data collected from user activity was stored locally on the user's device, securely encrypted and presumably resistant to unauthorized analysis by third parties. Apple's data retention and encryption policies appeared frequently in headlines a year ago when the company squared off against the FBI over the Bureau's insistence that the tech company provide aid in breaking the encryption on an iPhone during its investigation of the San Bernadino mass shooting on Dec. 2, 2015. As tech news site 'The Verge' reported, Apple CEO Tim Cook expressed the company's desire to protect the privacy of its users, stating the company has "a responsibility" to consumers to help protect their data and privacy. In iOS 10, Apple has broken with its tradition of relying solely on locally-encrypted data to customize the user experience, opting instead to use data aggregated across its vast population of users. This comes as Apple has significantly expanded the amount of data it collects on user activity, meaning that the software giant is collecting and storing user data on an unprecedented scale. Apple reps claim the company has taken steps to ensure the anonymity of the data they are collecting, though they have not provided many details on these practices.

…but they are using Differential Privacy to protect the data

At their WWDC in June, Apple execs briefly discussed the company's use of a cryptographic algorithm known as differential privacy to protect the large volume of data it is collecting from users. Differential privacy refers to the injection of randomized junk data, or noise, into a set of data to obscure the actual live data that is important to developers. For those adventurous souls who are not afraid of a deep dive into cryptography, Matthew Green from Johns Hopkins University posted an interesting write-up on his blog about the technology. Apple says that even though they are not collecting identifying or sensitive information from its users, they are aware of various techniques hackers might use to leverage traditional data sets, if compromised, to deduce the identity of users from otherwise anonymous data. Differential privacy is designed to protect user data from these types of attacks.

Unfortunately, Apple has not released many details on its implementation of differential privacy, leaving many security experts to wonder just how anonymous user data remains once it is collected. Apple has attempted to counter some of these concerns, insisting that, if such detail was released, hackers might leverage that information to bypass privacy safeguards.

You should still take steps to protect your information

Given the expansion of the amount of data Apple is collecting, privacy advocates are recommending users change some of the default functionality of iOS software to protect their information, even despite Apple's assurance that user privacy has not been compromised in this latest iteration of iOS. Tech news site 'ZDNet' recently published an article detailing steps every iOS 10 user should take to help maintain their privacy. Privacy advocates argue that in the Information economy, where user data is a valuable commodity, users should not take software vendor's claims regarding privacy protection for granted. Instead, they suggest, users should remain vigilant and always investigate published privacy policies for any software they might use.