Download Your Handout

Use mouse to click the dropdown arrow

Click to download

File Options View Help

Audio
Dashboard

Questions
Handouts:

Cybersecurity Awareness

2021 Webinar Series

GoToWebinar

Meet Your Speaker: Travis Street

- **President / CEO / Founder CTS**

- **Over 15 years working with IT and the Multifamily Industry**

- **Specialized in outsourced managed IT support, cybersecurity, and consulting services exclusively to Multifamily**

Cybersecurity Awareness and Multifamily: How to be a "Human Firewall" at your Properties

About CTS

Founded in 2001

15 Years in Multifamily

Managed IT support, consultation, and cybersecurity services to the multifamily industry

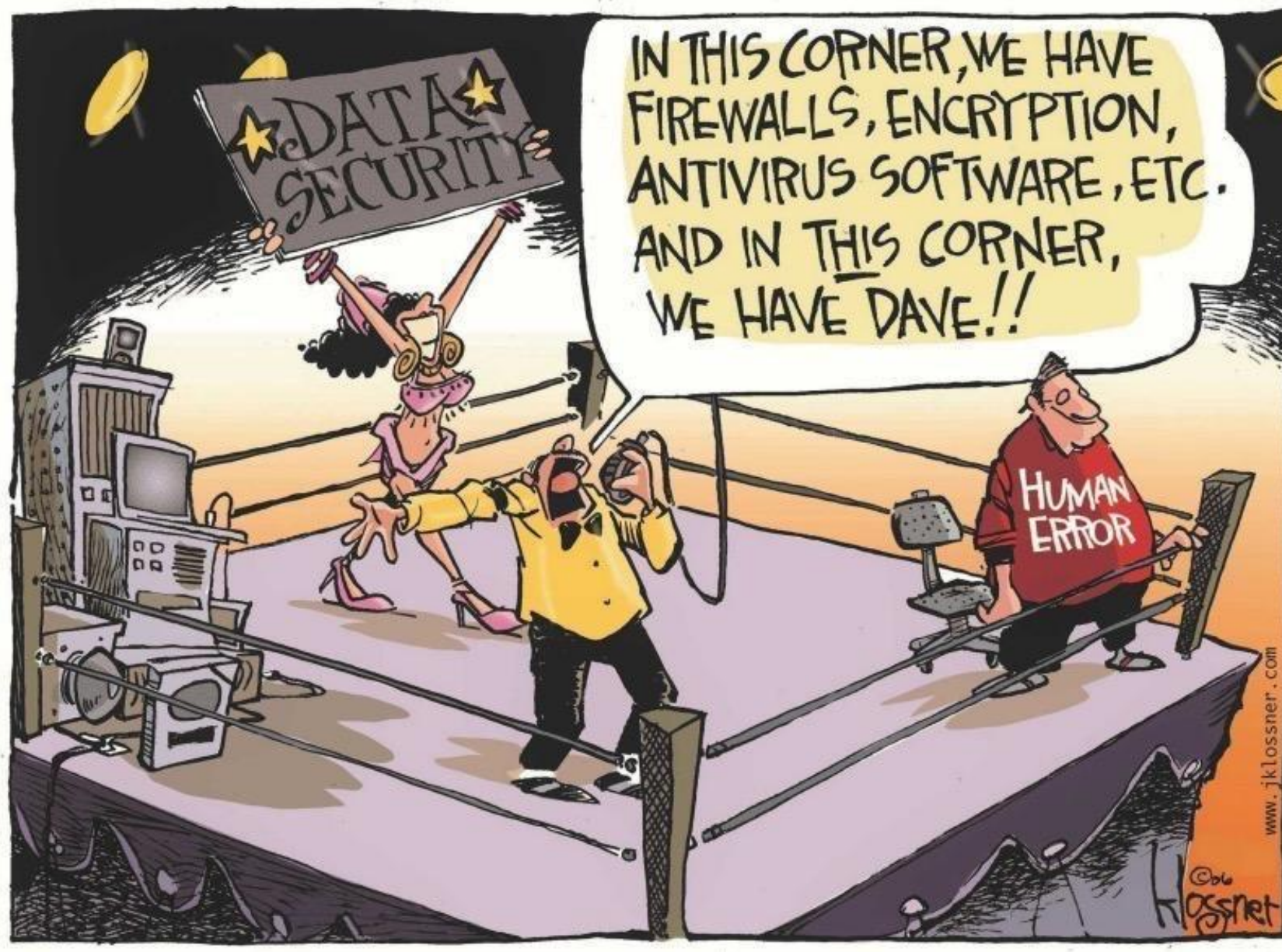24/7 Nationwide Remote and onsite Tech Support

Service Desk and Network Operations Center (NOC) based in Plano Texas

We Will Cover

This presentation will help educate you on basics of:

- What Cybersecurity Awareness means
- Why it is important
- Common pitfalls to be aware of
- How to avoid becoming a victim and become a "Human Firewall"

Why Is Cybersecurity Awareness Important to me?

Why Is Cybersecurity Awareness Important to me?

- Ever increasing number and sophistication of threats
- Help protect yourself and your assets
- Cost of incident downtime and recovery
- Company public image
- 43% of cyber attacks effect small businesses
- "You can have the best security in the world, but nothing will give you 100% protection. In this case, your staff are the last line of defense!" –Travis Street

What Knowledge and Skills are needed to be a "Human Firewall"?

"A **firewall** is a network security device that monitors traffic to or from your network. It allows or blocks traffic based on a **defined** set of security rules"

To be a "Human Firewall", you need:

- Stop & think mindset…and common sense
- Google Search (AKA Google-Fu)
- Basic understanding of how the attacks take place

Common Pitfalls – Malware, Phishing and Social Engineering

- Malware and Ransomware is software intended to harm your computer and systems

- Social Engineering is social techniques uses to illicitly obtain information or money via email or phone

- To gain a profit. Now a $8 Billion industry!

Common Malware

- Viruses
- Worms
- Trojans
- Ransomware
- Spyware

Other Threats

- Botnets
- Hacking
- Pharming
- Phishing
- Identity Theft
- Credit Card Fraud
- Wi-Fi Eavesdropping

- DoS/DDoS
- Rootkit
- Email Hoax
- Social Engineering
- Human Factor

Web Attacks – Scareware

- Tricks you into calling "Microsoft" and paying money to fix a fake issue
- They want remote access to your computer to "fix" the issue
- Web pages that look similar to real pages and want your login information. (Ex. Office 365, Facebook)

⚠ WARNING!

YOUR COMPUTER MAY BE INFECTED:

System Detected (2) Potentially Malicious Viruses: Rootkit.Sirefef.Spy and Trojan.FakeAV-Download. Your Personal & Financial Information MAY NOT BE SAFE.

To Remove Viruses, Call Tech Support Online Now:

1(866) 627-4049

(High Priority Virus Removal Call Line)

Your IP Address: 216.57.72.238 | Generated on 03-11-2014 | Priority: Urgent

---

🛈 Error   Please install Flash Player HD to continue   (Required)

Scareware Prevention and Elimination

- It can happen even if you have good security software installed – can originate from streaming podcast sites, web advertisements

- Don't click anything!

- Ctrl – Alt –Delete is your friend! Kill the task.

- If that isn't possible, hold down power button on computer to power cycle your computer

- If scareware is still present after reboot, call your IT support team

Ransomware

- $2 Billion industry a year
- Survey: 51% of companies victim
- Encrypts your files and holds the key until you pay in Bitcoin
- Costs average $2,500
- Backups with long retentions
- Few firewalls or antivirus can help block
- "Friendly" tech support phone number to call to help you pay the ransom

Ooops, your files have been encrypte

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other accessible because they have been encrypted. Maybe you are recover your files, but do not waste your time. Nobody can rec our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely a not so enough time.
You can decrypt some of your files for free. Try now by click But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the pri Also, if you don't pay in 7 days, you won't be able to recover y We will have free events for users who are so poor that they c

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, cli Please check the current price of Bitcoin and buy some bitcoin click <How to buy bitcoins>.
And send the correct amount to the address specified in this w After your payment, click <Check Payment>. Best time to chec

t will be raised on
1970 17:00:00
Time Left
00:00:00

r files will be lost on
1/7/1970 17:00:00
Time Left
:00:00:00

Send $600 worth of bitcoin to this a
₿ bitcoin
ACCEPTED HERE
12t9YDPgwueZ9NyMgw519p7AA8i

Check Payment

Physical Threats

- Shoulder surfing

- Tailgating

- External drives – avoid free thumb drives!

- Desktop Security – lock your screen!

- Always ask Vendors for Credentials and verify the purpose of their visit, especially if they are working on telecom, door access control or other amenities with technology

Cell/Mobile Devices

- Just as vulnerable
- Use AV
- Use cell network, not free WiFi
- Stay updated
- Don't side load apps
- Don't jailbreak/root

Property Management Companies Are a Target of Phishing!!

- Many times, hackers learn the organization structure of your company from your website
- They study your vendors and processes
- They use stolen information from the dark web to create realistic signatures/emails

Common Types of Phishing seen by Management companies

- Fake emails from executives, regionals to property staff requesting "favors"
- Fake emails from your IT department saying your credentials are expired
- Fake invoices from vendors with suspicious attachments
- Fake documents being sent from property scanner
- Fake Voicemails attachements
- Extortion emails (rare but very effective!)

Phishing Example

Phishing Example

First American Title closing@fnf.com sent you Receipt-Escrow Deposit #-
00788560-005-HO5 3-19-2021.pdf

You can download these files now or until **3/26/2021.**
Questions? Ask First American (audreyabawatson@hotmail.com)

Download files

Here's what they sent you
1 item • 113 KB

Receipt-Escrow Deposit #-00788560-005-HO5 3-19-2021.pdf
113 KB

Office 365

A document has been sent through One Drive. Click the Access
Document button below and Log in with your email account to
view it.

From: Christian Garner <info@comcast4gtextmessages.com>
Sent: Monday, November 23, 2020 12:29 PM
To: █████████████████
Subject: Gift Cards

> EXTERNAL EMAIL** Use extreme caution when clicking any links or attachments, as they may have viruses or other malicious content, and NEVER provide your password, even if prompted to do so. If unsure, send the email to
> help@avantiresidential.com for review.

████ a quick message before it skips my mind again. I need you to purchase some gift cards from the store today. We intend to reward some staffs with it Reply and let me know how soon you can get this done. Also, please keep this confidential pending the time we announce it.

Regards,
--
Sent from Comcast 4G Wireless

Greetings!

I have got two not really pleasant news for you.
I have been monitoring your internet activities for some time by now.

The only person to blame in this situation is you, since you are a big fan of adult websites and also have got an uncontrollable desire to indulge yourself with another orgasm.
Simply speaking, all your porn websites search requests have become a key to access your device.
The thing is that I work in a company that provides services related to security and performance of email providers, including ▬▬▬▬▬.com as well.

I can easily decrypt passwords of users, access their chat history and online traffic with help of cookie-files.
I have decided to analyse users traffic related to adult websites and adult content.
I was truly shocked to discover that nearly 75% of users regularly access porn websites or participates in sex chats.

I have filtered out the worst perverts from the list. Yeah, you are one of them. Not everyone chooses to watch such hardcore videos...
Basically, I have infected your device with one of the best Trojan viruses in the market. It was relatively easy, since I have access to your email address (EMAIL).
Since this spyware is driver-based, then I can constantly update its signatures, so that no antivirus can detect it.
While digging through your hard drive, I have saved your entire contact list, social media access, chat history and media files.

One week ago, I have montaged a videoclip, which shows you masturbating on one side of the screen and on the other side a porn video that you were watching at that moment of time - recently this type of exotic stuff is really popular on the internet!
Don't worry, I will need just a few mouse clicks in order to share this video with your entire contact list and upload it to some porn website, like Bigle.
I believe that you would not like this to happen, since a long holiday season is just about to start soon -
just imagine the number of silly jokes and loud laughter that would get provoked by your video all over the neighbourhood bars and pubs...

I am offering a simple and reasonable solution:
All you need to do is transfer an amount equivalent to $1950 (USA Dollars) to my bitcoin wallet and we both forget about this silly story forever.
All your data and this video will be deleted by me once and for all. You have my honest word!
You've got to agree, this amount is really insignificant. Just imagine how much time and resources I have spent to get this done...
If you don't know how to operate the cryptocurrency - you can always search for assistance online via google.com. It is that simple.

Here is my bitcoin wallet (BTC): 16fbeN6D5JkTU7Ywh8zdAPoQWD6TzN1ZSf

You have exactly 2 days (48 hours) from the moment of opening this email.
I still don't receive the required amount of money, then your videoclip will be automatically sent to all your contact list and uploaded to public websites.

Extortion Example

What Can You Do?

- Passwords & Password Manager
- Two-factor authentication
- Separate business & personal emails/passwords
- Utilize security software
- Keep OS & programs updated
- Encryption
- **Be The Firewall!**
- Call your IT team or CTS anytime you have doubts

Password Security Tips

- Keep your passwords private - Do not write or email!

- Use passwords of at least 12 (twelve) characters

- Use a combination of characters (ex. 3v4%Y}!)

- Don't use dictionary words

- A strong password should look random

- Change regularly (ex. 30, 60, 90 days)

Password Creation How To

Follow These Steps	Example
Think of a phrase or sentence with at least eight words.	I Want To Put A Dent In The Universe
Remove all but the first letter of each word in your phrase	IWTPADITU
Replace several of the upper-case letters with lower case ones	iWtpADitU
Now substitute a number for at least one letter	iWtpAD1tU
Finally, use a special character to replace a letter or two	iW+pAD1tU!

Threats now compared to a few years ago…

Q & A

Thank You!

If you need help or guidance, reach out to me anytime at **travis@ctsmultifamily.com** or call **888.266.9715**

Upcoming Webinars 2021

Up Next: 5/27/21 at 1:00 PM CST
10 Tips for Exceptional Customer Service
with Wesley Aleshire

Register:
edge2learn.com
epmsonline.com

edge2learn

www.edge2learn.com

Questions?