Office Practicum
2017 User Conference

2017 OP UC

Powering a More
Profitable Practice

Gone Phishing

Presented by: Mike Matlack, President & CIO

By the end of this session, you will understand various **internet threats**, and ways to help **keep you** and **your practice safer**.

Why is this important?

Overview

- Threats
  - Phishing
  - Ransomware
  - Vishing
  - SMishing
  - Public Wifi
- Password safety
- Tools to keep your team safe
- Resources to keep your practice informed

Why would crooks come after me?

- To get **$$** from you
- To use your computer to **attack other computers**
- To get your **sensitive data** so they can sell it on the **black market**

TECHNOLOGY NEWS | Wed Sep 24, 2014 | 2:24pm EDT

Your medical record is worth more to hackers than your credit card

How much more?
10 to 60 times more!

Threats: Phishing

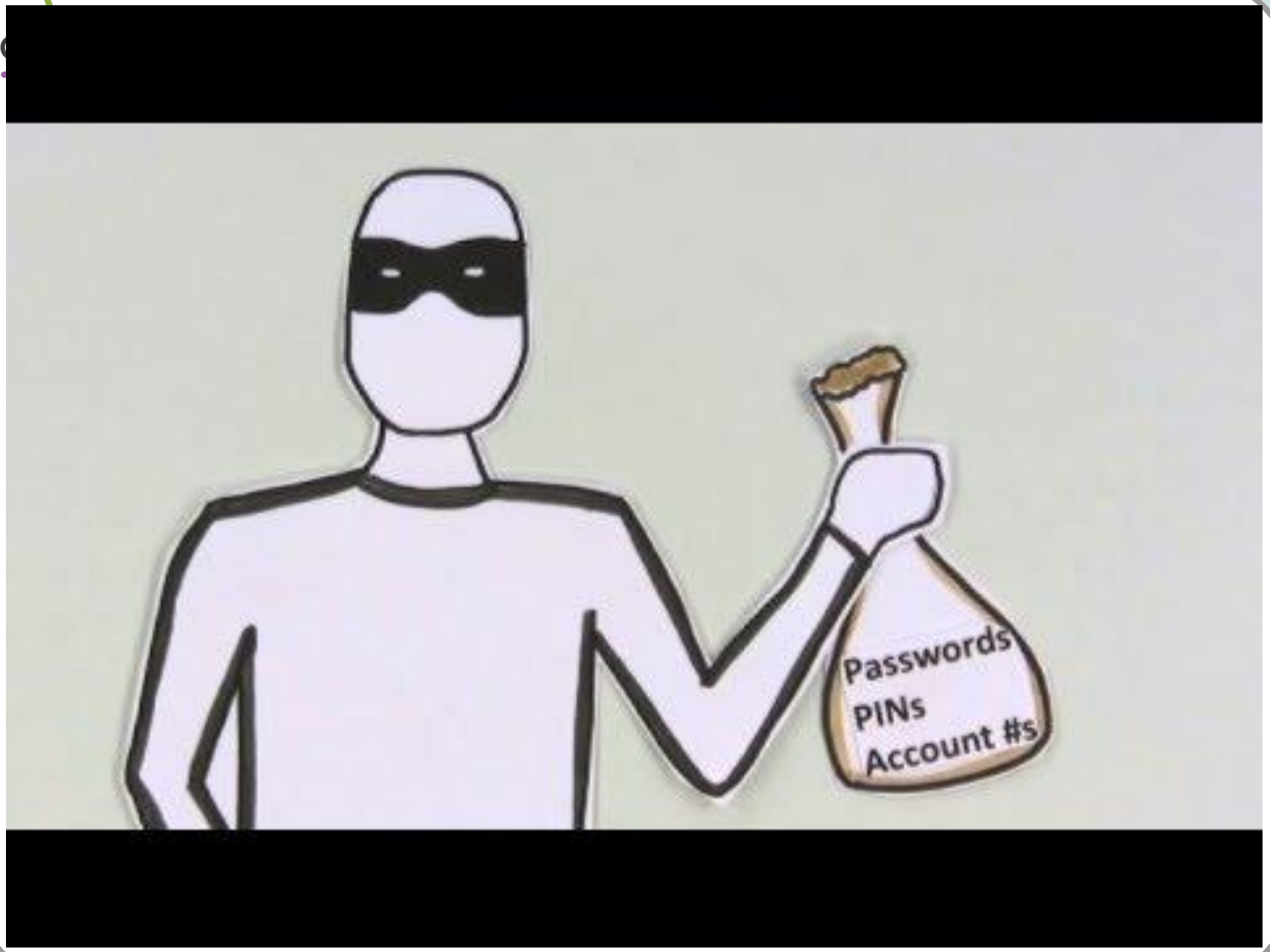
Phishing

What is it?

- A crook sends an email with a **link** that looks innocent
- If you click on the **link**, it would take you to a site that tries to **steal your sensitive information**

OR

- A crook sends an email with an **attachment** that looks innocent
- If you open the **attachment**, it would install **malware** on your computer (we'll talk more about this later in *ransomware*)


Passwords
PINs
Account #s

A phishing email can be as simple as a “survey” asking what street you grew up on.

Even non-sensitive information can be used to gain access into your personal life.

Phishing - How to recognize it

An example email

Hello!

As part of our security measures, we regularly screen activity in th
Google system. We recently contacted you after noticing an issue
on your account

Our system detected unusual Copyrights activity linked to your
Google account . please follow the line bellow to fill the Copyrigh
Law form:

https://apps.google.com/user/hub http://www.NotTheSafestPlaceToBe.com

Note: If you don't fill the application, your account will be
permanently blocked.

Regards,

Google Copyrights Department

name?

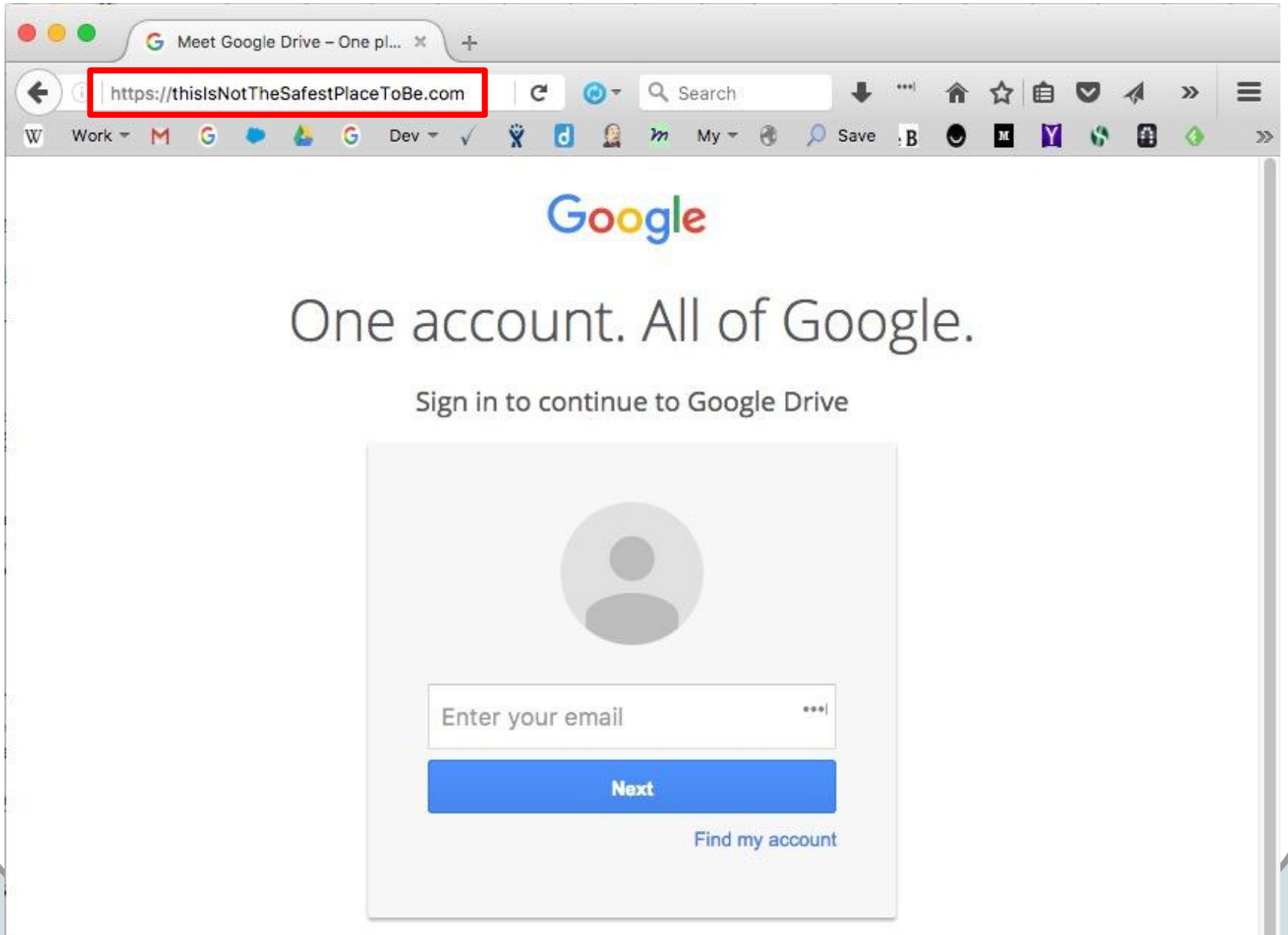
spelling

link

threat

known company

Phishing


Meet Google Drive – One pl...
https://thisIsNotTheSafestPlaceToBe.com
Search
Work
Dev
My
Save
Google
One account. All of Google.
Sign in to continue to Google Drive
Enter your email
Next
Find my account

Phishing

How to defend against it

"The best way to protect yourself from phishing attacks is to never click on any links or open any attachments sent to your email"

And since that is close to impossible

- Verify email with senders … "did you send me this?"
- Delete suspicious email and ignore suspicious attachments (including ads in sites you know and trust)
- Be careful of emailed instructions ("please send your password", "disable security on your computer to install this new application").

Phishing

What is it?

- A crook sends an email with a **link** that looks innocent
- If you click on the **link**, it would take you to a site that tries to **steal your sensitive information**

OR

- A crook sends an email with an **attachment** that looks innocent
- If you open the **attachment**, it would install **malware** on your computer (we'll talk more about this later in *ransomware*)

Threats: Ransomware

malware

The Latin root word *mal* means *bad* or *evil* :-(

Hidden software that steals your information or remotely controls your machine, or spies on you.

Ransomware

What is it?

- A crook sends an email with an **attachment** that looks innocent
- If you **open** the attachment, it would install **malware** on your computer
- The malware then **encrypts** your files, **locks** your operating system, or **prevents** your computer from even booting
- The ransomware creators then require you to **pay a fee**, e.g. $500, to get **access** to your computer
- The fee often has to be paid with **bitcoin**

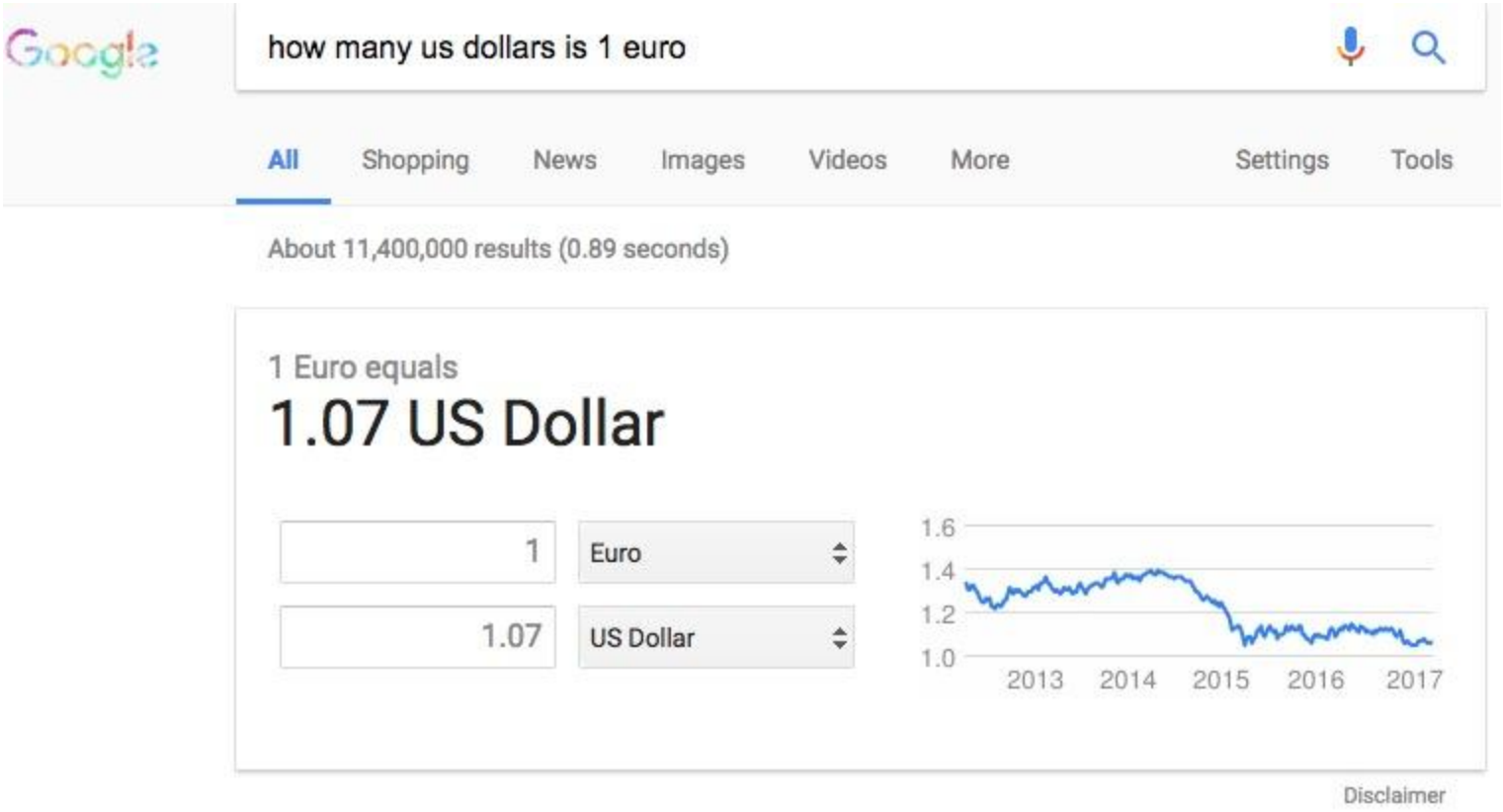
The ransomware creators provide lots of help files on how to pay with bitcoin, and often have a support desk to help you pay your fee!?!?!?!

bitcoin

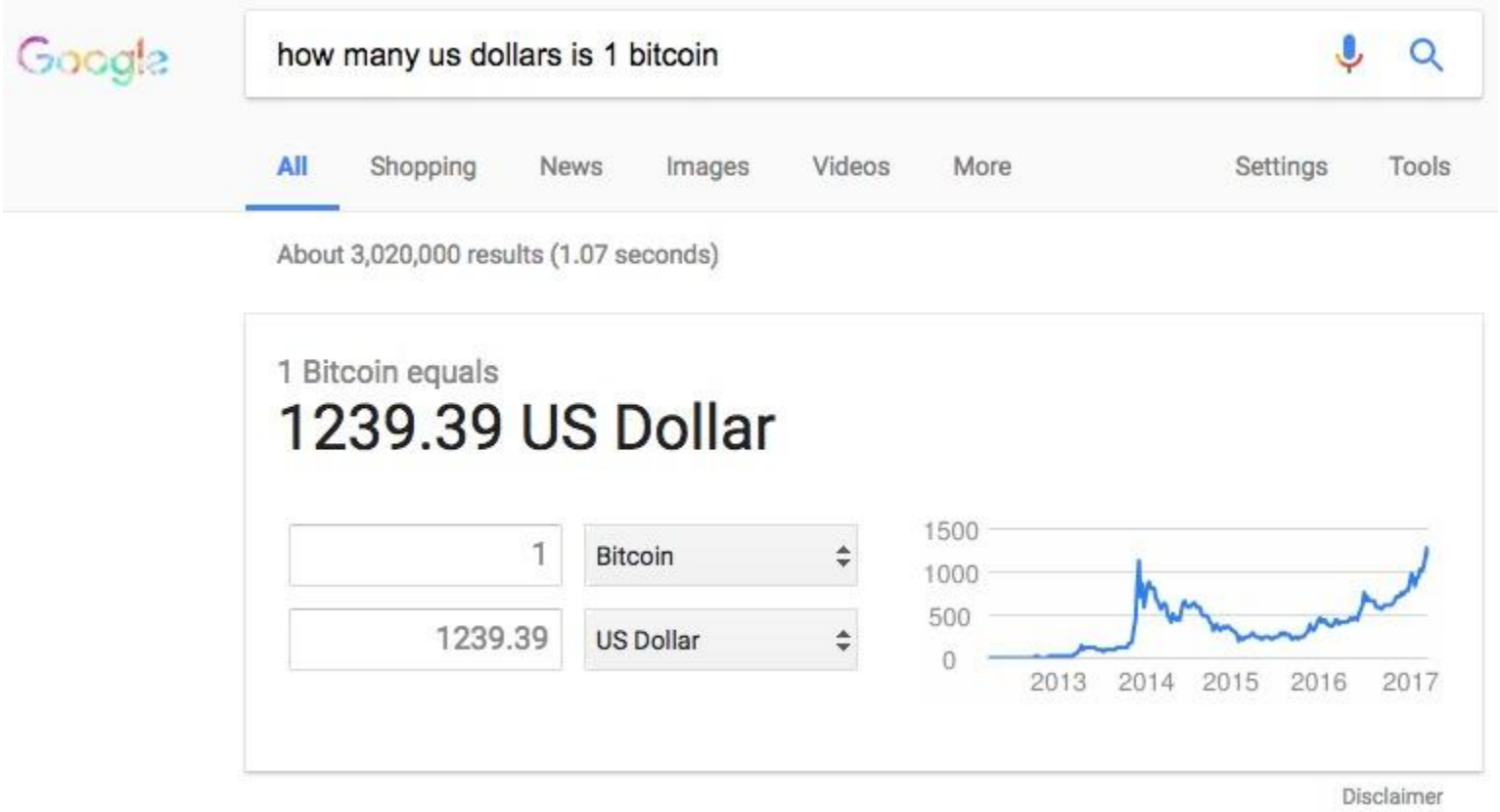
a type of **digital currency** in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, **operating independently of a central bank**

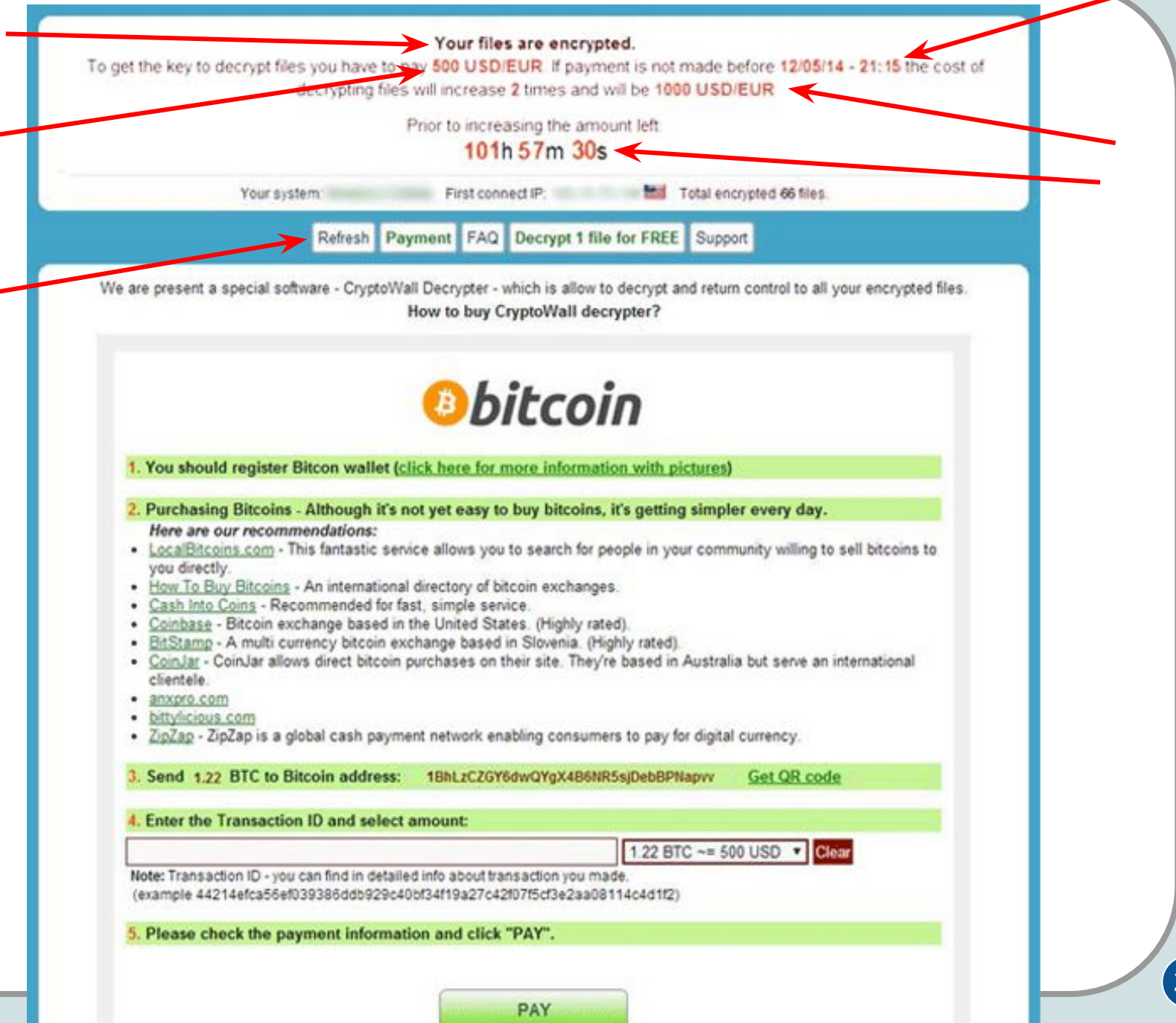
...and it's often untraceable

Google ‘how many us dollars in 1 euro’



Google ‘how many us dollars in 1 bitcoin’

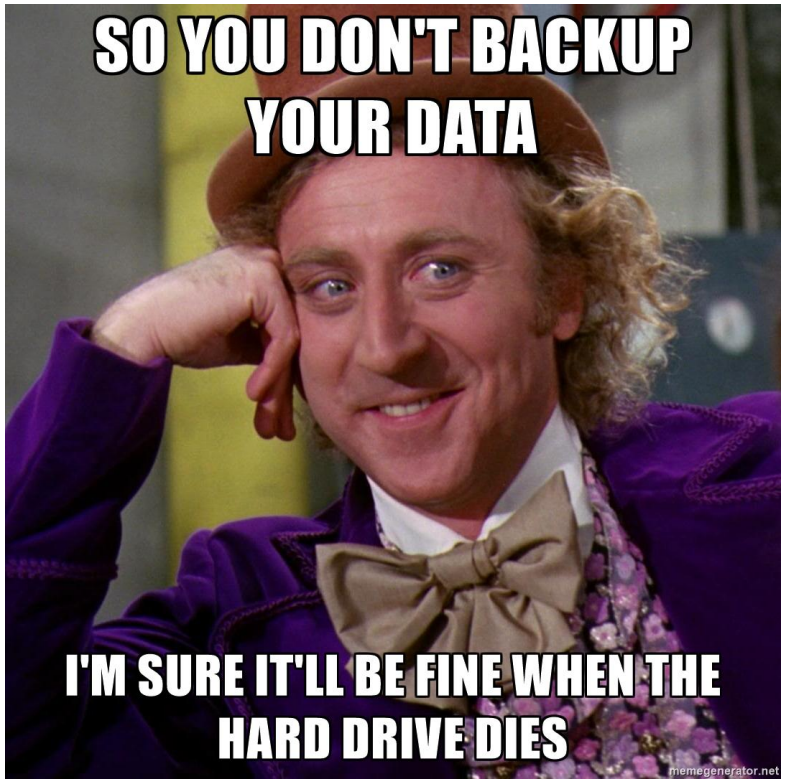



Your files are encrypted.
To get the key to decrypt files you have to pay 500 USD/EUR If payment is not made before 12/05/14 - 21:15 the cost of decrypting files will increase 2 times and will be 1000 USD/EUR
Prior to increasing the amount left:
101h 57m 30s
Your system: First connect IP: Total encrypted 66 files
Refresh
Payment
FAQ
Decrypt 1 file for FREE
Support
We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.
How to buy CryptoWall decrypter?
bitcoin
1. You should register Bitcon wallet (click here for more information with pictures)
2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.
Here are our recommendations:
LocalBitcoins.com - This fantastic service allows you to search for people in your community willing to sell bitcoins to you directly.
How To Buy Bitcoins - An international directory of bitcoin exchanges.
Cash Into Coins - Recommended for fast, simple service.
Coinbase - Bitcoin exchange based in the United States. (Highly rated).
BitStamp - A multi currency bitcoin exchange based in Slovenia. (Highly rated).
CoinJar - CoinJar allows direct bitcoin purchases on their site. They're based in Australia but serve an international clientele.
anxpro.com
bittylicious.com
ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.
3. Send 1.22 BTC to Bitcoin address: 1BhLzCZGY6dwQYgX4B6NR5sjDebBPNapvv Get QR code
4. Enter the Transaction ID and select amount:
1.22 BTC ~= 500 USD
Clear
Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)
5. Please check the payment information and click "PAY".
PAY

Ransomware

Top 10 ways to protect yourself

1. Backup your data
2. Backup your data
3. Backup your data
4. Backup your data
5. Backup your data
6. Backup your data
7. Backup your data
8. Backup your data
9. Backup your data
10. Backup your data



Why? So if you get hit with ransomware, you do not have to pay them to get your data back.

Ransomware

How to protect yourself

1. **Backup** your data
2. **Delete** suspicious email and **ignore** suspicious attachments
3. Use a **private server** or service (local office server, Google Drive, Dropbox) to **share** files with a coworker.
4. Open suspicious documents in an **online service**, like Google Docs.
5. Keep your operating system **up to date and patched**
6. Install **security software**
7. If you are infected, **disconnect** (see Ransomware, Hostage Rescue Manager)

Ransomware

Should you pay?

- It can be expensive: $300-$600
- Law enforcement will recommend you don't pay
- But…it's difficult to put a cost on your baby videos, 10 years of digital photos, tax returns, practice data, etc.

So…

- It's OK to pay, but better if you don't have to
- Take the proper precautions **NOW** (backup!) so you don't have to make that decision

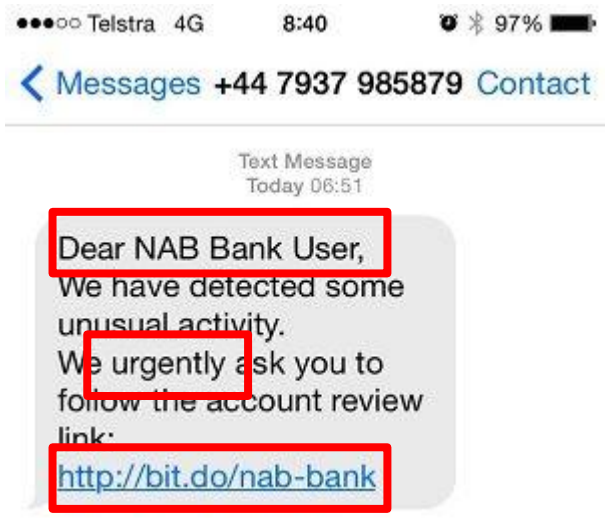
Threats: Vishing & SMishing

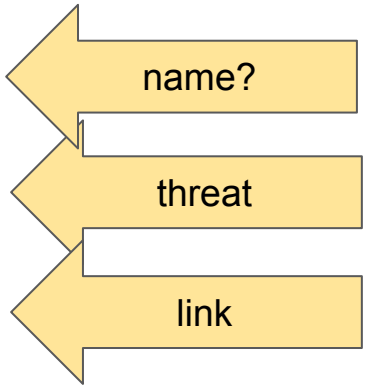
Vishing - Voice based phishing

SMishing

Phishing via text messaging

- Texting = Short Message Service (SMS) -> SMishing
- Same rules for Phishing apply here





Threats: Public Wifi


Free
Wi Fi

Public wifi

Why is it a threat?

- It can be easy for someone to **snoop** on your **unsecured browsing.**
- There is **public information** available about "how to see what others are doing on an unsecured network", e.g. this article from 2014 (i.e. a "How to" guide to perform "man-in-the-middle" attacks). Anyone can easily find and experiment with this information.
- If your device is not protected, others can **connect to your hard drive.**
- **Any device** is vulnerable, your laptop, smartphone or tablet.

Public wifi

How to keep safe

- Turn off sharing on your device (instructions in the presentation notes for Windows and Mac)
- Connect to websites using **https**: when it is available

Https

Internet protocol that encrypts the information you send over the internet (like your credit card) and makes it more secure.

Public wifi

How to keep safe

- Turn off sharing on your device
- Connect to websites using **https**: when it is available
- Require users who connect to your company network to use a **Virtual Private Network** (VPN)

VPN (Virtual Private Network)

group of computers
networked together
over a public network—
namely, the internet

But be aware, some companies are trying to cash in on “privacy wars”

Public wifi

How to keep safe

- Turn off sharing on your device
- Connect to websites using **https**: when it is available
- Require users who connect to your company network to use a **Virtual Private Network** (VPN)
- Verify the **wifi network** you are connecting to is **legitimate**. Anyone can create a wifi hotspot and call it whatever they want, e.g. “Free Atlantic City Wifi”

Questions

Password safety

Passwords

Why are they important?

OK, that was a trick question 😁

Choose a complex password

For 20 Years the Nuclear Launch Code at US Minuteman Silos Was 00000000

Karl Smallwood - TodayIFoundOut.com
11/29/13 7:00am · Filed to: WEAPONS

334.5K 110

Today I found out that during the height of the Cold War, the US military put such an emphasis on a rapid response to an attack on American soil, that to

https://gizmodo.com/for-20-years-the-nuclear-launch-code-at-us-minuteman-si-1473483587

Passwords

How to choose one

- Don’t use short (less than 8 characters) or common passwords. Password crackers use long lists of common passwords when trying to learn yours. Are any of these familiar?

  123456

  password

  12345678

  qwerty

  12345

  123456789

  football

Passwords

How to choose one

- Use a long, nonsensical, phrase including numbers and punctuation, e.g. Wi$hUponABanj0.
- Make a memorable, unusual, sentence: "I am a 7-foot tall metal giant", and use the first letter of each word with punctuation: "Iaa7-ftmg"
- Use a tool to generate (and remember) passwords for each site you log into

Passwords - Don't reuse!

Usernames and passwords are vulnerable

Even if you use complex passwords and don't share them among sites, usernames and passwords are still vulnerable from phishing and hacking.

One Solution: Two step authentication

Passwords

Two Step Authentication

Step 1: Login like you normally would (something you know)

Step 2: generate a key with your cell phone, or insert a security key (something you have)

Passwords

Two step authentication

Sign In

Enter login credentials

Email address: jd@gmail.com

Password: Wi$hUponABanj0

Sign In

Enter security key

Code:

Passwords

Two Step Authentication

When you sign in on your home computer you can indicate not to use two-step authentication on it, then you just need your password.

But other locations will still require two-step authentication to keep you safe.

Tools to keep your team safe

Tools to share with your team

- Hardware encrypted portable external hard drive for offsite backup. Get a pair, alternate one for nightly backup, the other to take off site that night.
- Email that checks for phishing (like GMail)
- Password managers (like Lastpass) to generate strong passwords, and remember them for you … but read this to understand tradeoffs
- Browser extensions, like HTTPS Everywhere (for Chrome, Firefox and Opera) that make sure you are using HTTPS where it is available
- Browser settings, like those in google Chrome, that post warnings if you browse to a phishing sites.

Resources to inform your practice

Resources

- This presentation!
- Helpful infographics (look here for details on how to print out these great Creative Commons posters)
  - Internet safety rules to teach children :-)
  - Common Phishing attacks
- HIPAA Training (OP uses http://www.hipaasecurenow.com/ which costs $49/year for organizations of up to 10 employees)
- Guidelines on mobile privacy
  - http://lifehacker.com/the-privacy-enthusiasts-guide-to-using-android-1792432725
  - http://lifehacker.com/the-privacy-enthusiasts-guide-to-using-an-iphone-1792386831
- References at the end of this presentation

Conclusion

Actions … what now?

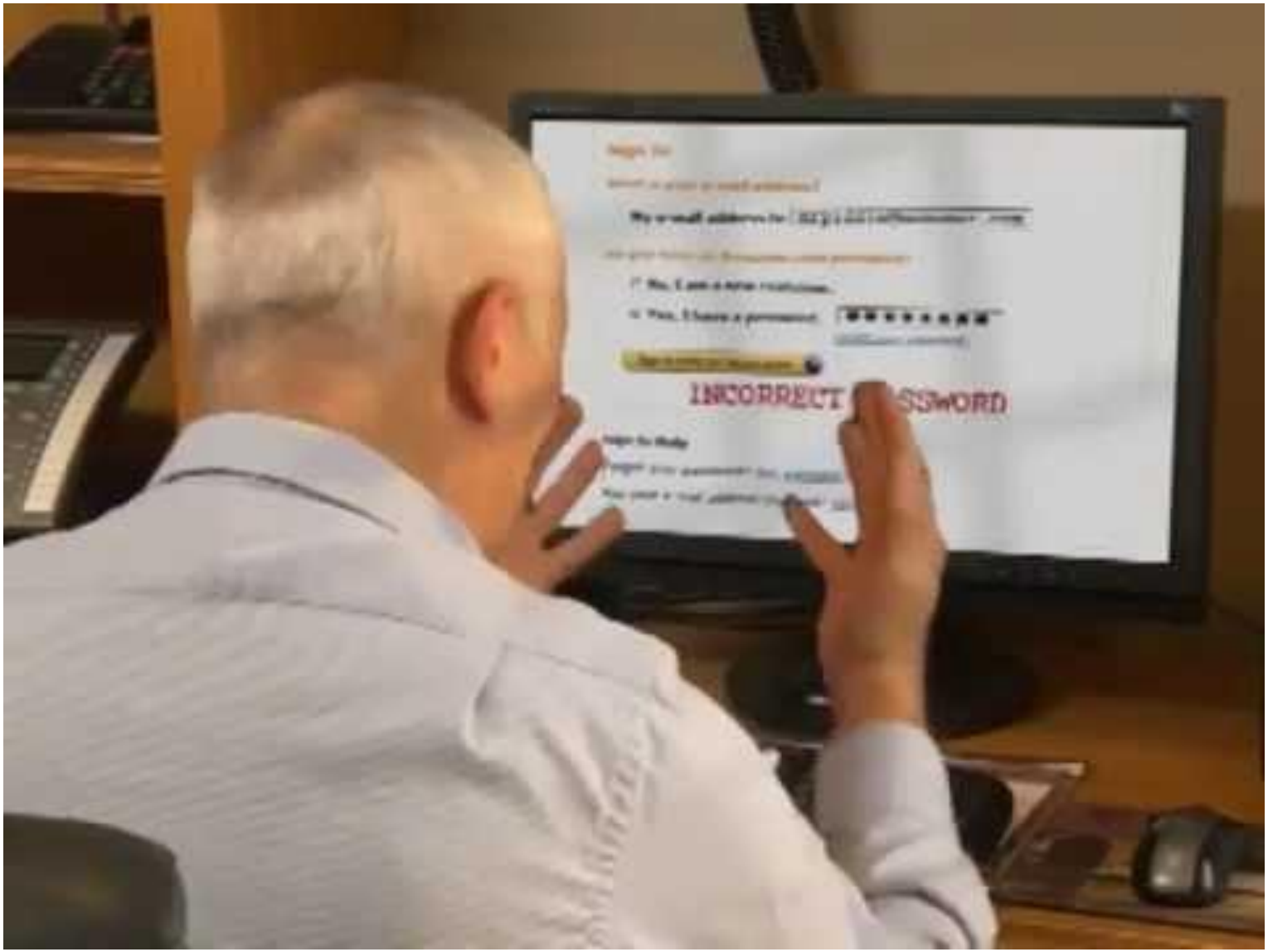
- **Backup** all critical data
- Make sure your **servers** are running up-to-date and patched operating systems (OP does this for cloud users)
- Make sure your **workstations** are running up-to-date and patched operating systems
- Use **2 step authentication** when available
- Make sure you are **browsing** the internet **securely** (https)
- **Share** this **presentation** with your team
- **Print and post** the infographics around your office
- Make sure your practice has **HIPAA training** each year, and make it easy to do
- **Share** the **tools** you learn about with your team at work and your family at home

Conclusion

In this session we learned

1. What potential threats are out there
2. What tools you can use to increase safety
3. What you can do to help your practice stay safe

If time … a tool you should NOT use :-)



Questions

References

- Medical records worth to criminals: http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924
- Phishing: https://ssd.eff.org/en/module/how-avoid-phishing-attacks
- Tech support scammers: https://www.wired.com/2017/03/listen-tech-support-scam-calls-bilk-millions-victims/
- Ransomware: https://heimdalsecurity.com/blog/what-is-ransomware-protection/#ransomwaretargets
- Ransomware: https://www.wired.com/2016/05/4-ways-protect-ransomware-youre-target/
- Ransomware Hostage Reference Manual
- Public wifi: https://lifehacker.com/5576927/how-to-stay-safe-on-public-wi-fi-networks or https://fieldguide.gizmodo.com/how-to-stay-safe-on-public-wifi-1779464400
- Two step authentication: https://plus.google.com/+LaurenWeinstein/posts/avKcX7QmASi
- Common passwords: http://www.telegraph.co.uk/technology/2016/01/26/most-common-passwords-revealed---and-theyre-ridiculously-easy-to/
- Healthcare workers prioritize helping people over information security (disaster ensues) https://boingboing.net/2016/06/28/healthcare-workers-prioritize.html
- Medical devices are the next security nightmare, yikes! https://www.wired.com/2017/03/medical-devices-next-security-nightmare/
- How quickly things change (added this after my “final” slides) https://www.engadget.com/2017/03/31/when-the-s-in-https-also-stands-for-shady/
- Billboards and stores can track you!

Thank You!

Please tell us how we did

Navigate to this session in the App

- Rate The Session
- Take Short Survey
- Or Take Paper Survey