Cybersecurity and Protecting Your Practice

T-BONES Texas Orthopedic Administrators Society

Acentec
Improving Medical Practice Performance®

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

HIPAA® SECURITY SUITE
Your Key to HIPAA Compliance®

Cybersecurity and Protecting Your Practice

Jeff Mongelli

CEO & Founder

Acentec, Inc.

Member of:

FBI Infragard

HEALTHCARE Intelligence

Federal Cyber Health Working Group

HSIN
HOMELAND SECURITY INFORMATION NETWORK

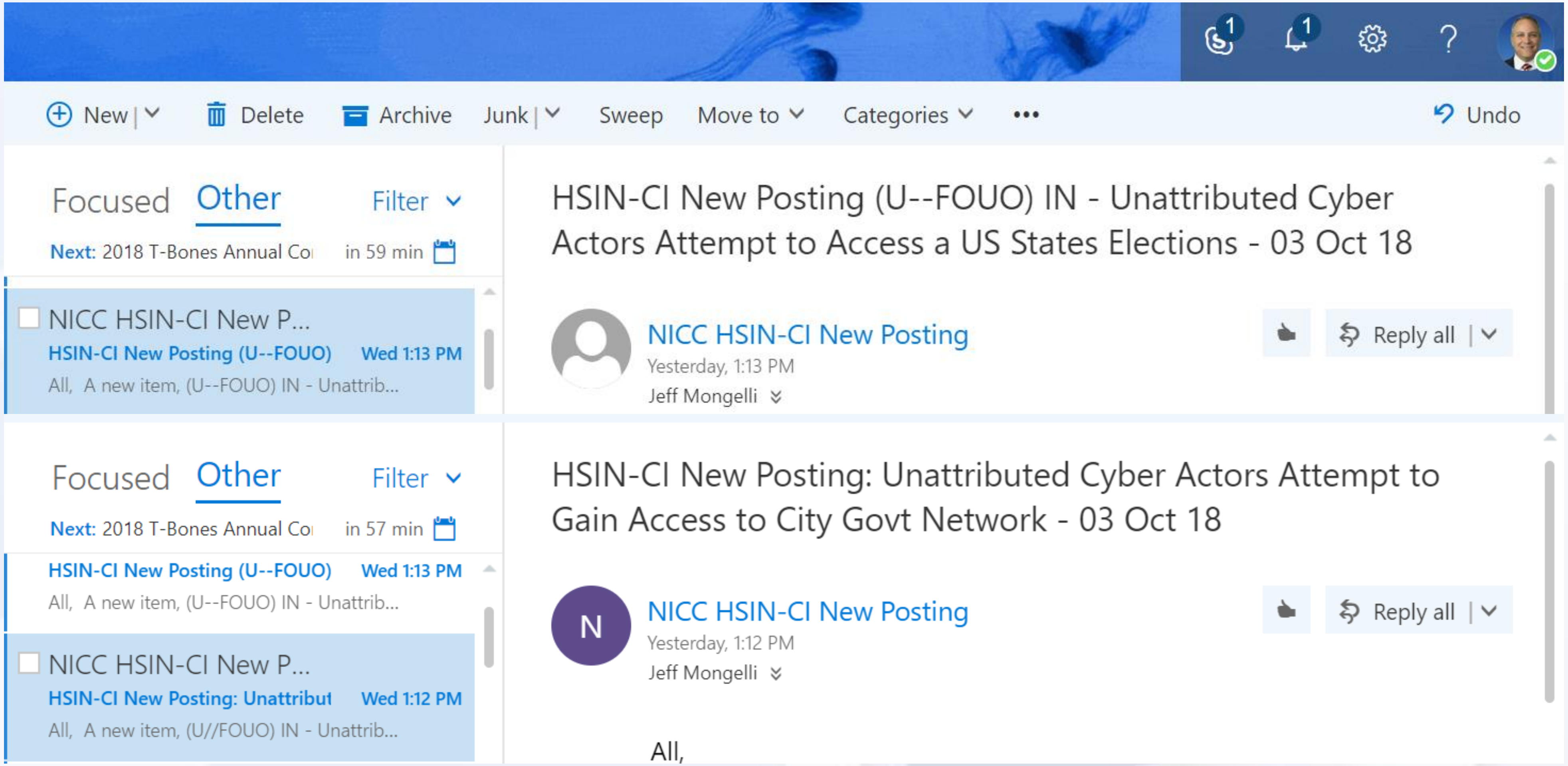
Acentec
Improving Medical Practice Performance®

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

HIPAA® SECURITY SUITE
Your Key to HIPAA Compliance®

Outline for today

1. The latest in cyber threats
2. What to look out for
3. What you can do to protect yourself


New | Delete Archive Junk | Sweep Move to Categories ••• Undo
Focused Other Filter
Reply all

Next: 2018 T-Bones Annual Co in 59 min

☐ NICC HSIN-CI New P...
HSIN-CI New Posting (U--FOUO) Wed 1:13 PM
All, A new item, (U--FOUO) IN - Unattrib...

HSIN-CI New Posting (U--FOUO) IN - Unattributed Cyber Actors Attempt to Access a US States Elections - 03 Oct 18

NICC HSIN-CI New Posting
Yesterday, 1:13 PM
Jeff Mongelli

Next: 2018 T-Bones Annual Co in 57 min

HSIN-CI New Posting (U--FOUO) Wed 1:13 PM
All, A new item, (U--FOUO) IN - Unattrib...

☐ NICC HSIN-CI New P...
HSIN-CI New Posting: Unattribut Wed 1:12 PM
All, A new item, (U//FOUO) IN - Unattrib...

HSIN-CI New Posting: Unattributed Cyber Actors Attempt to Gain Access to City Govt Network - 03 Oct 18

N NICC HSIN-CI New Posting
Yesterday, 1:12 PM
Jeff Mongelli

All,

Acentec
Improving Medical Practice Performance®

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

HIPAA® SECURITY SUITE
Your Key to HIPAA Compliance®

Lord & Taylor
KOHL'S
expect great things
THE HOME DEPOT
The Vitamin Shoppe
Stein Mart
kmart
macy's
Kroger
Toys R Us
The Container Store
CVS pharmacy
Walgreens
Panera
Walmart
Whole Foods Market
myfitnesspal
H-E-B
Publix
BED BATH & BEYOND
BAKERY
TARGET
Avenue
BEST BUY
COSTCO WHOLESALE
SEARS
Sam's Club

APOLLO

2018 – Sales engagement company Apollo exposed 200 million records of US individuals and companies.

EXACTIS

2018 - Data aggregator Exactis exposed 340 million records of US citizens and companies.

US population is approx. 328 million.

CYBER THREAT ORIGINS

Acentec
Improving Medical Practice Performance®

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

HIPAA® SECURITY SUITE
Your Key to HIPAA Compliance®

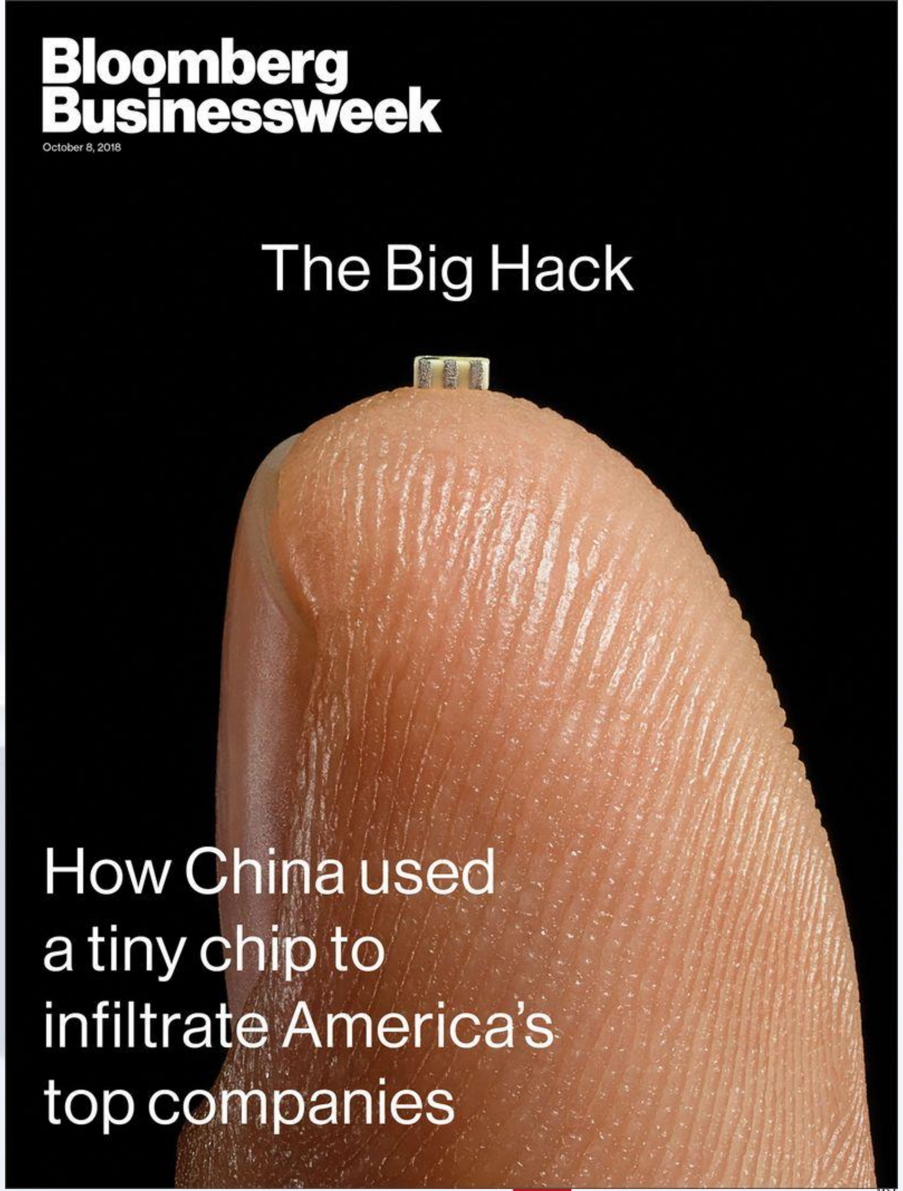
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
Shadow Brokers

Why are they winning?

The Chip Dilemma

Announced Oct. 4, 2018

Over 30 companies and agencies known to be infected since 2015 including Amazon, Apple, Feds.



Bloomberg Businessweek

October 8, 2018

The Big Hack

How China used a tiny chip to infiltrate America's top companies

Acentec

Improving Medical Practice Performance®

Arthur J. Gallagher & Co.

BUSINESS WITHOUT BARRIERS™

HIPAA SECURITY SUITE

Your Key to HIPAA Compliance®

New Ways We’re Being Attacked

- While watching the following video, think about how this type of attack could be used against you, your organization, and your clients.

What’s New In Cyber Threats?

Acentec
Improving Medical Practice Performance®

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

HIPAA®
SECURITY SUITE
Your Key to HIPAA Compliance®

New Threats and Evolving Old Ones

- VPNFilter
- Ransomware and more
- Advanced Spear Phishing

VPNFilter

VPNFilter

- Malware (MiTM) that targets common home routers
- The list of targeted devices has grown so large it's better to look at excluded devices
- Approaching 1 million vulnerable devices
- Significant in that it represents a new focus

VPNFilter – What it can do

- Intercept ALL data traffic and manipulate it
  - Drain your bank account,
  - Access your hospital and connected sites
  - Access your EHR
- Takes control of your connection
- Install any malware payloads

VPNFilter – How to stop it

- VPNFilter doesn’t need your invitation.
- Here’s the recommended protocol:
  - Factory reset your router
  - Re-install clean firmware
  - Manually re-configure router
  - Disable remote management
  - Change default access information

VPNFilter – Here’s what most people will do

- Nothing – unaware or lack skills
  - For that reason, this vulnerability will be with us for years.
- Replace the router
  - Newer routers can automatically update firmware

Ransomware

- Malware that encrypts your data and forces you to pay a ransom to regain access.

Ransomware By The Numbers

- SamSam, WannaCry, Petya, NotPetya, GandCrab and now Ryuk
- Unlimited variants thanks to MAAS
- Global cost estimate:
  - $5 Billion in 2017, $11.5 Billion by 2019

From Cybersecurity Ventures report

Acentec
Improving Medical Practice Performance®

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

HIPAA® SECURITY SUITE
Your Key to HIPAA Compliance®

Ryuk Ransomware – Aug 2018

- Similar to SamSam – most prolific healthcare ransomware
- Tailored to each victim
- Built for small scale attacks
- Masquerades as Russian but origins are North Korea (most likely Lazarus)

Ransomware Evolution

- Slowing growth of shotgun attacks
- Expansion of more targeted attacks
    - More advanced tactics
        - Credential theft
        - Social engineering
    - Target organizations with sensitive data who have $$$$ to pay

Other Attacks

DRAGON NATURALLYSPEAKING by NUANCE

EQUIFAX

- **NotPetya -** Nuance & Banco De Chile in May - $10MM stolen, 500 servers destroyed.
- **Doxware -** Ransomware that notifies patients
- **Apache Struts -** Web server & IoT (Equifax – 150M)
- **Malvertising -** Visiting (legitimate) hacked sites
- **Crypto-Mining -** Your PC to generate crypto-currency.

Other Attacks

- Medical Devices and IoT
  - Only **35%** of healthcare delivery organizations encrypt traffic on IoT devices.
  - **39%** of manufacturers said attackers have taken control of devices.
  - **38%** of care delivery organizations said inappropriate therapy/treatment had been delivered to patients because of an insecure medical device.

From the Ponemon Institute

Threat Vectors

Acentec

Improving Medical Practice Performance®

Arthur J. Gallagher & Co.

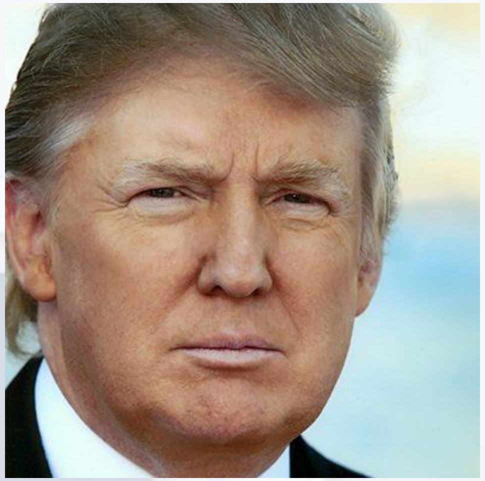
BUSINESS WITHOUT BARRIERS™

HIPAA SECURITY SUITE®

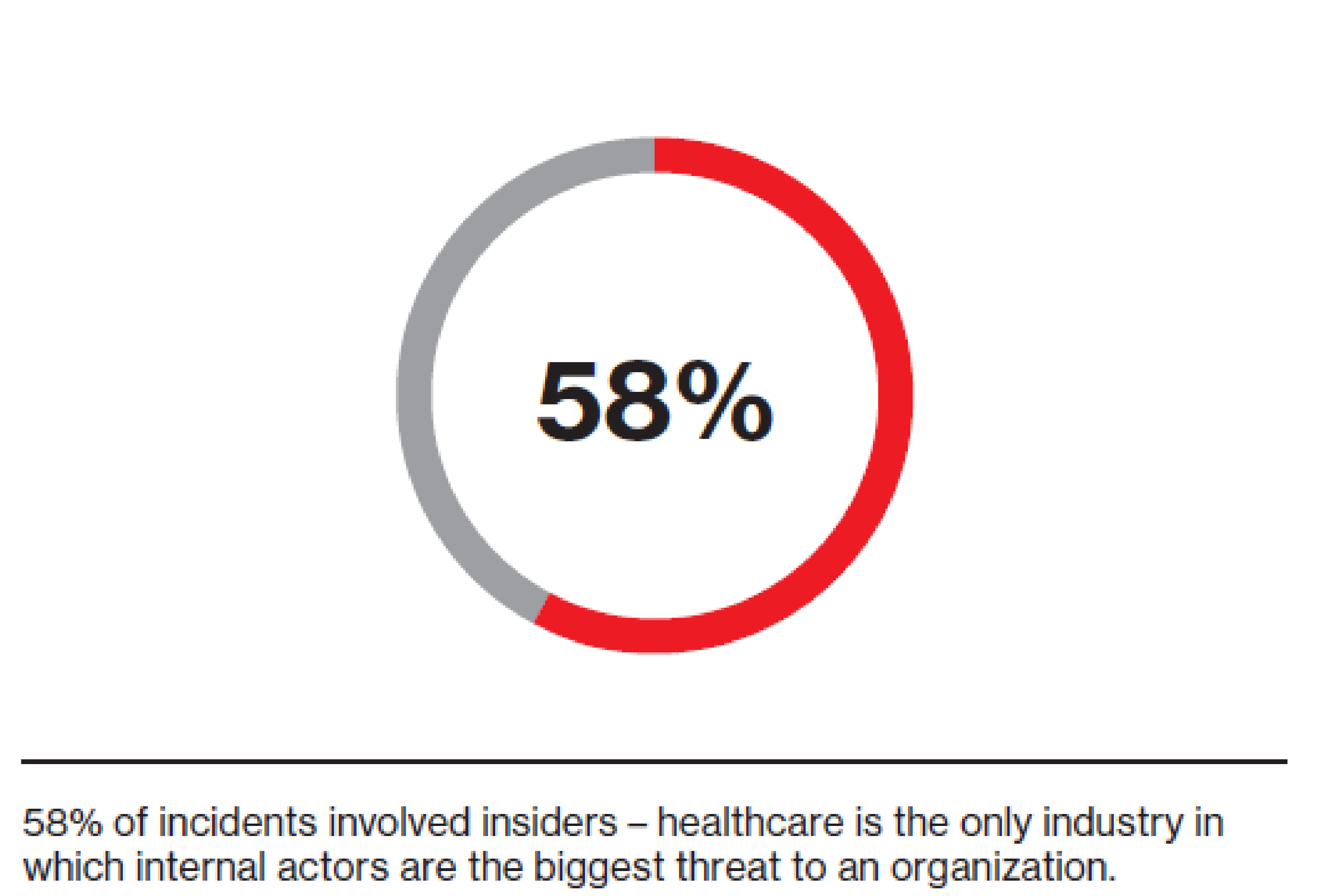
Your Key to HIPAA Compliance®

Who is a bigger threat?

✓



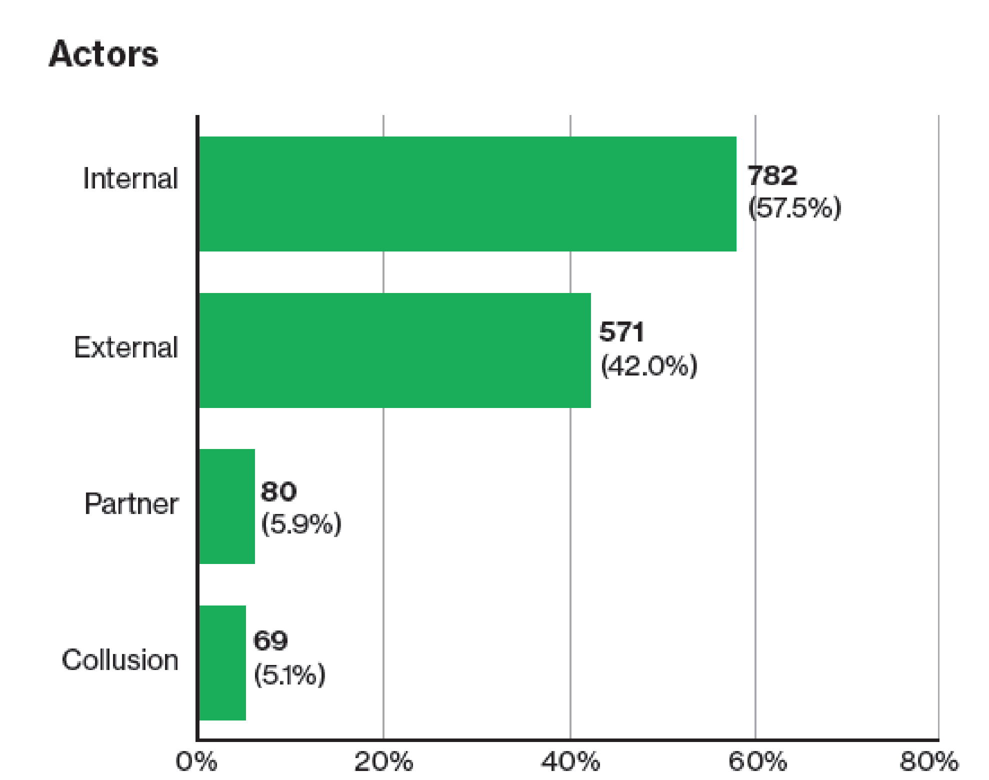
The Enemy Within



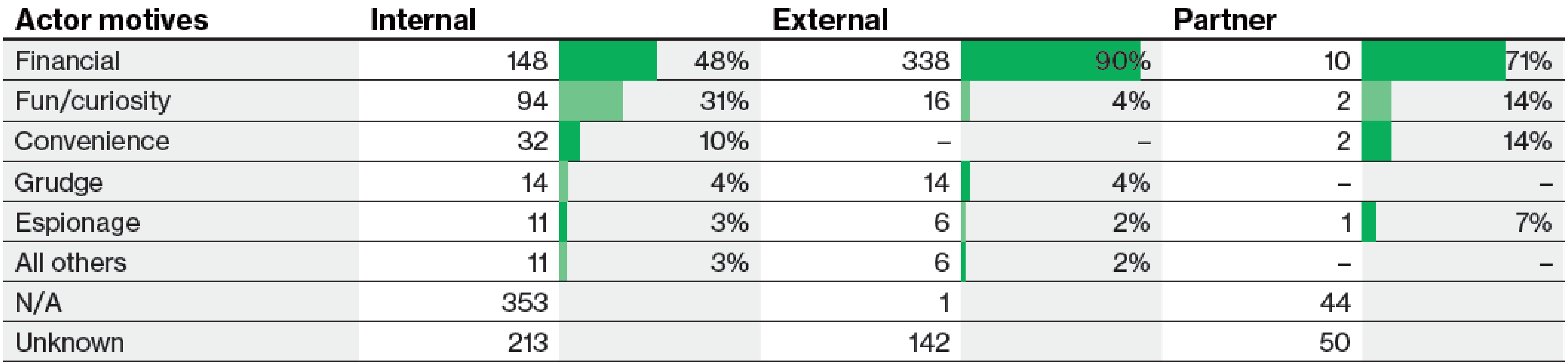
58% of incidents involved insiders – healthcare is the only industry in which internal actors are the biggest threat to an organization.

2018 Verizon PHI Data Breach Report

What’s their motivation?



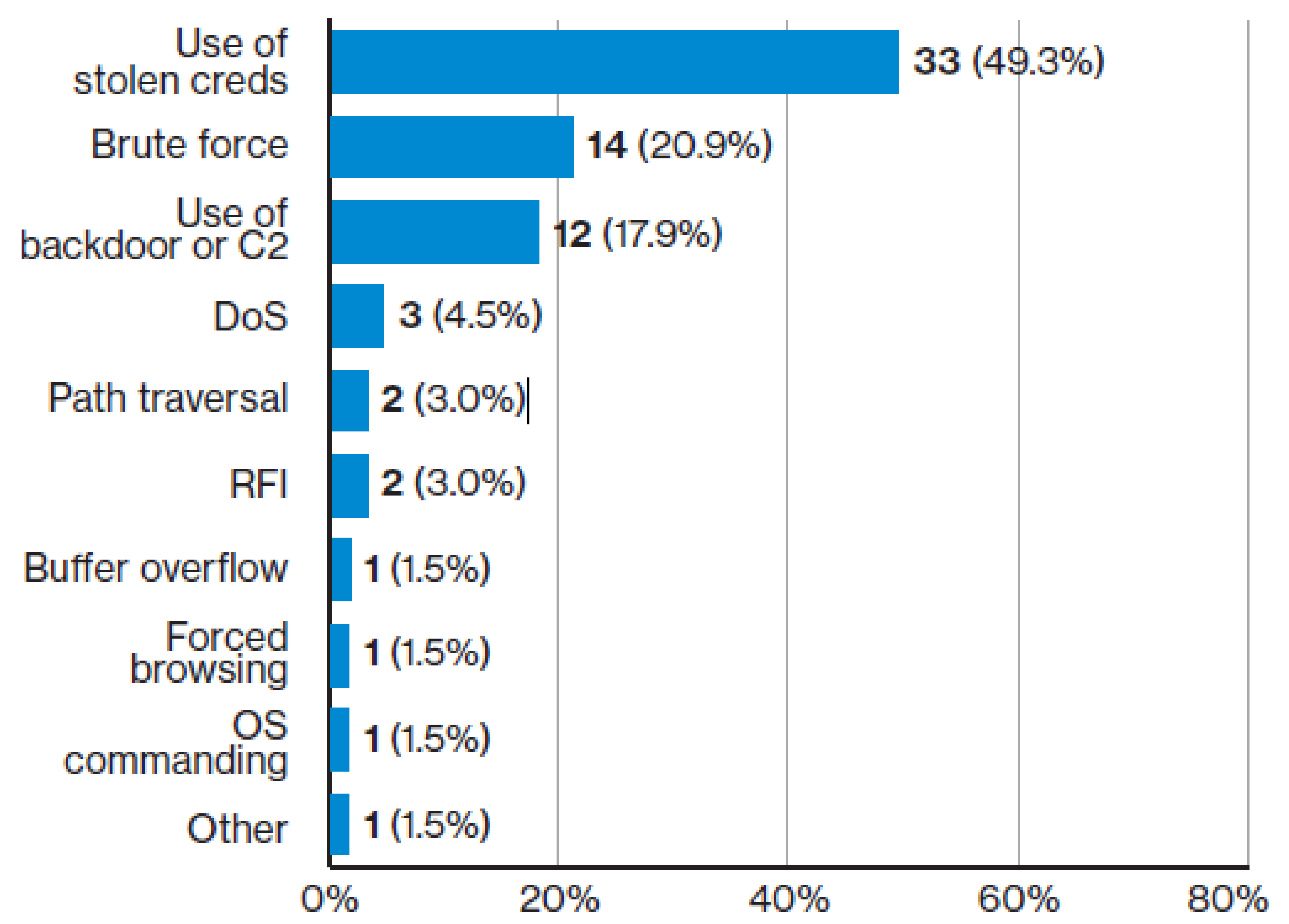
2018 Verizon PHI Data Breach Report



Actor motives	Internal		External		Partner	
Financial	148	48%	338	90%	10	71%
Fun/curiosity	94	31%	16	4%	2	14%
Convenience	32	10%	–	–	2	14%
Grudge	14	4%	14	4%	–	–
Espionage	11	3%	6	2%	1	7%
All others	11	3%	6	2%	–	–
N/A	353		1		44	
Unknown	213		142		50	

How Hackers Get In

2018 Verizon PHI Data Breach Report



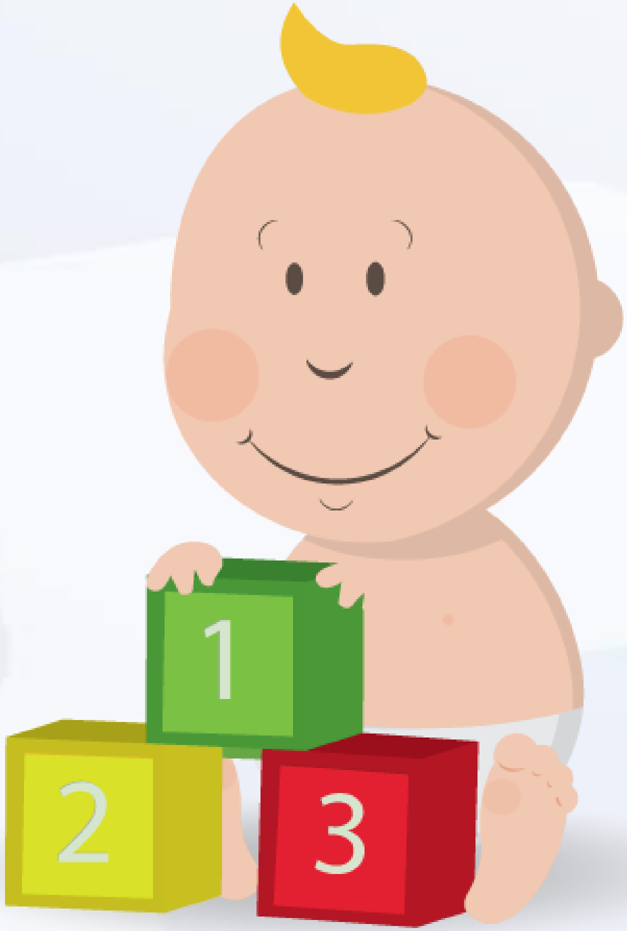
Acentec
Improving Medical Practice Performance®

Phishing Attacks

- Phishing Schemes
- Spear Phishing Schemes
- Vishing Schemes
- Targeted Hacks

Vishing Attacks

- Use of social media to target individuals and organizations.
- Attacks commonly combine emails and phone calls (including personal cell phones).
- Caller ID is spoofed to look familiar
- **Vector – email, phone, mail, fax**



Three Scenarios

Acentec
Improving Medical Practice Performance®

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

HIPAA SECURITY SUITE®
Your Key to HIPAA Compliance®

Scenario 1: Vishing

- You receive an email from a new patient with a pdf attachment called “my_medical_records.pdf”
- The patient calls to confirm you received it and if you can open it to confirm….

Scenario 2 – Spear phishing (vishing)

- Staff member went to pay a bill on line by a clicking link in an email from the lender.

Acentec
Improving Medical Practice Performance®

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

HIPAA® SECURITY SUITE
Your Key to HIPAA Compliance®

Scenario 2 – Spear phishing (vishing)

- Browser was redirected to an attack site, began looping an audio recording and “locked” her PC.
- She then got a call on her cell phone from the payment company saying her identity had been stolen and that she should buy an insurance policy for $200 – all phony.

Scenario 3 – “Blue Water” Spear phishing

- Accounting staff receives an email request for a pending wire from a legitimate vendor.
- They receive an email from the CFO authorizing the wire to the new bank information.

Scenario 3 – “Blue Water” Spear phishing

- Staff REPLIES to an existing email thread with the bank authorizing the release of the wire.
- $300,000 went into the wind – last trackable record was Germany.

Scenario 3 – "Blue Water" Spear phishing

- **FBI alert** (Sept 2017) – bank fraud in central states targeting doctors
  - Numerous incidents where an individual called to inquire about bank balances and used social engineering to answer security questions and withdraw thousands of dollars.

Reducing Your Risk

Acentec
Improving Medical Practice Performance®

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

HIPAA® SECURITY SUITE
Your Key to HIPAA Compliance®

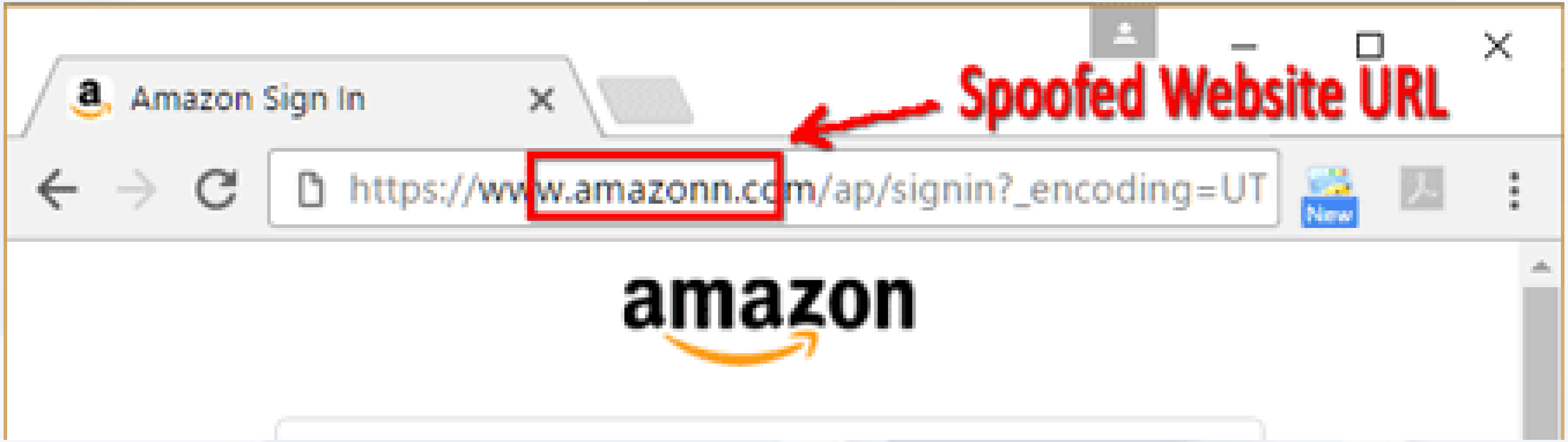
Spotting Spoofing

Acentec
Improving Medical Practice Performance®

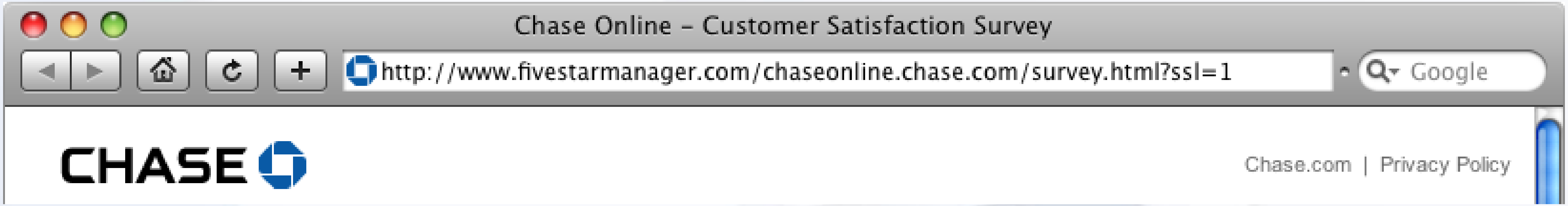
Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

HIPAA® SECURITY SUITE
Your Key to HIPAA Compliance®

Spoofed Websites



Spoofed Websites



Chase Online – Customer Satisfaction Survey

http://www.fivestarmanager.com/chaseonline.chase.com/survey.html?ssl=1

Spoofed Emails

Acentec

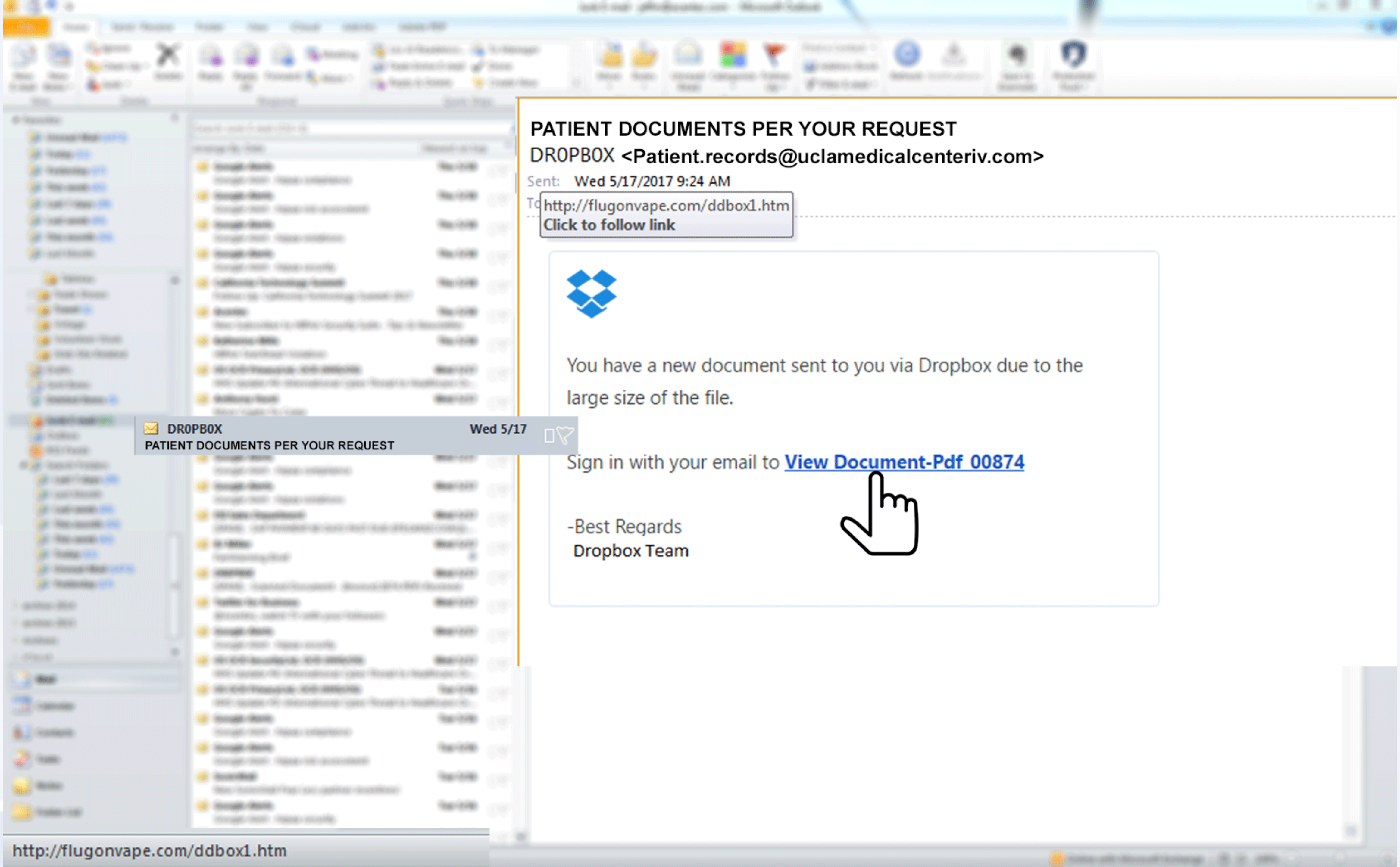
Improving Medical Practice Performance®

Arthur J. Gallagher & Co.

BUSINESS WITHOUT BARRIERS™

HIPAA® SECURITY SUITE

Your Key to HIPAA Compliance®



DR0PB0X
PATIENT DOCUMENTS PER YOUR REQUEST
Wed 5/17

PATIENT DOCUMENTS PER YOUR REQUEST

DR0PB0X <Patient.records@uclamedicalcenteriv.com>

Sent: Wed 5/17/2017 9:24 AM

To

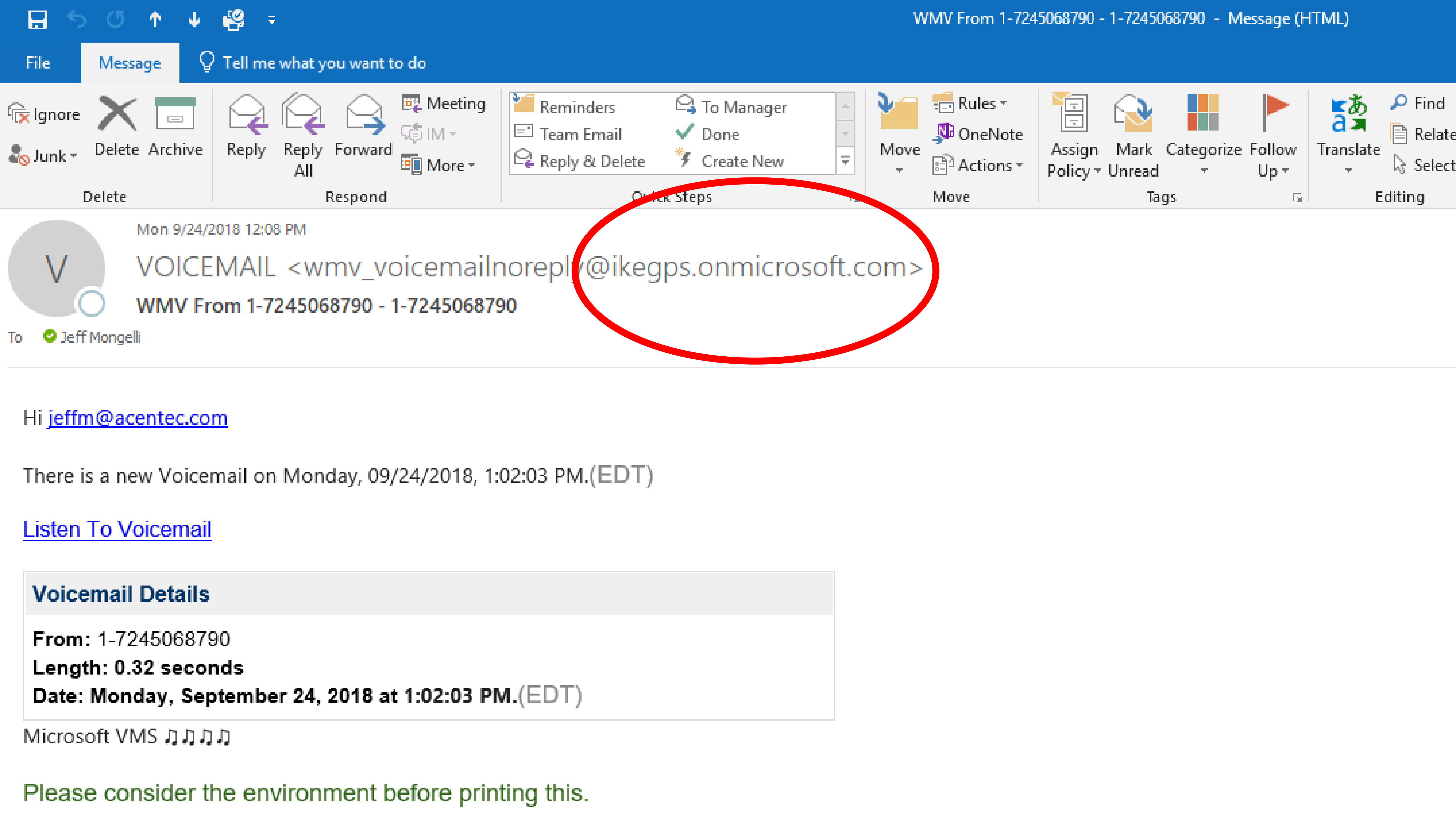
http://flugonvape.com/ddbox1.htm
Click to follow link

You have a new document sent to you via Dropbox due to the large size of the file.

Sign in with your email to **View Document-Pdf_00874**

-Best Regards
Dropbox Team

http://flugonvape.com/ddbox1.htm



Mon 9/24/2018 12:08 PM

VOICEMAIL <wmv_voicemailnoreply@ikegps.onmicrosoft.com>

WMV From 1-7245068790 - 1-7245068790

To Jeff Mongelli

Hi jeffm@acentec.com

There is a new Voicemail on Monday, 09/24/2018, 1:02:03 PM.(EDT)

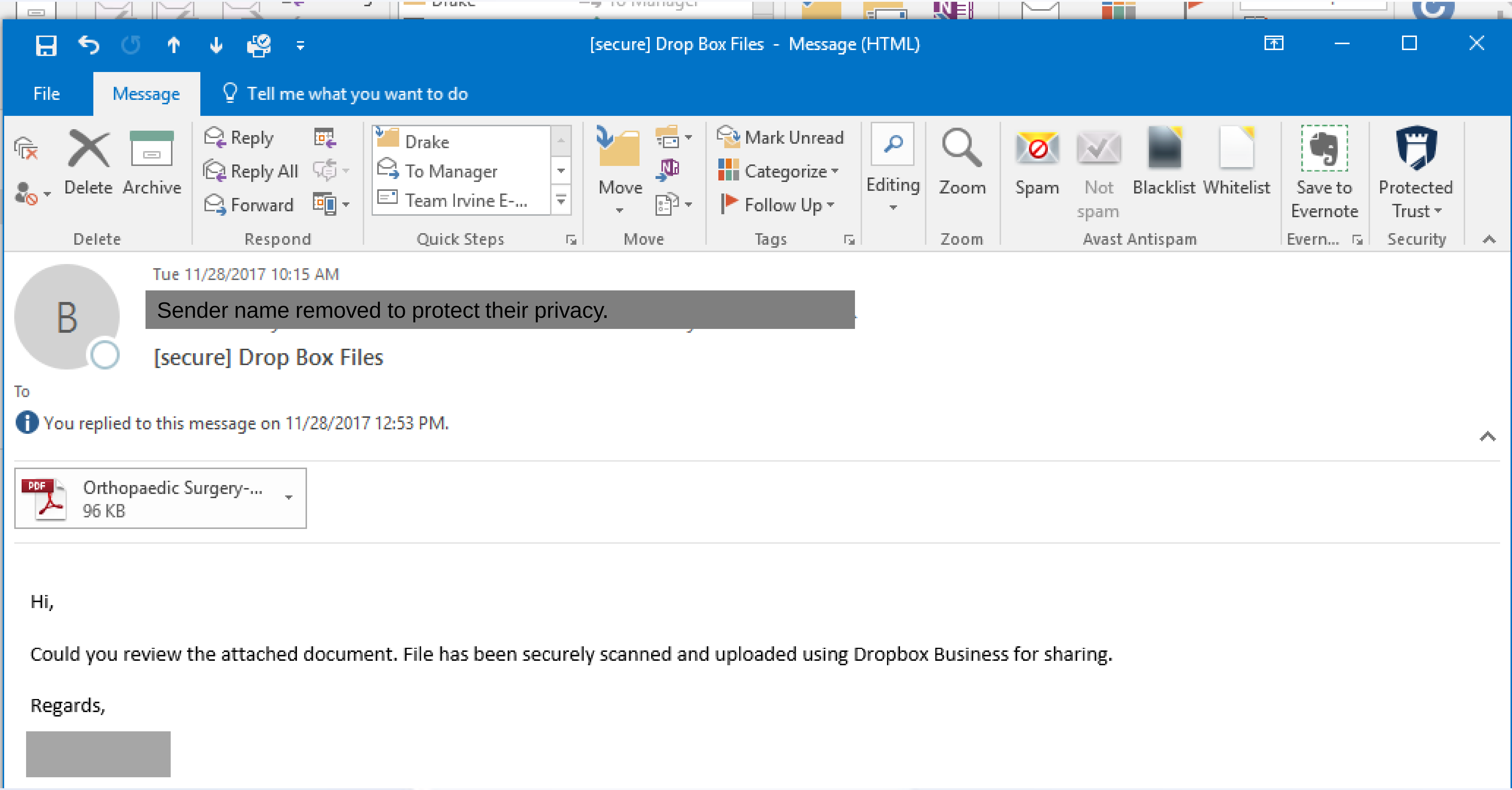
Listen To Voicemail

Voicemail Details

From: 1-7245068790
Length: 0.32 seconds
Date: Monday, September 24, 2018 at 1:02:03 PM.(EDT)

Microsoft VMS ♫♫♫♫

Please consider the environment before printing this.



Tue 11/28/2017 10:15 AM

Sender name removed to protect their privacy.

[secure] Drop Box Files

To

You replied to this message on 11/28/2017 12:53 PM.

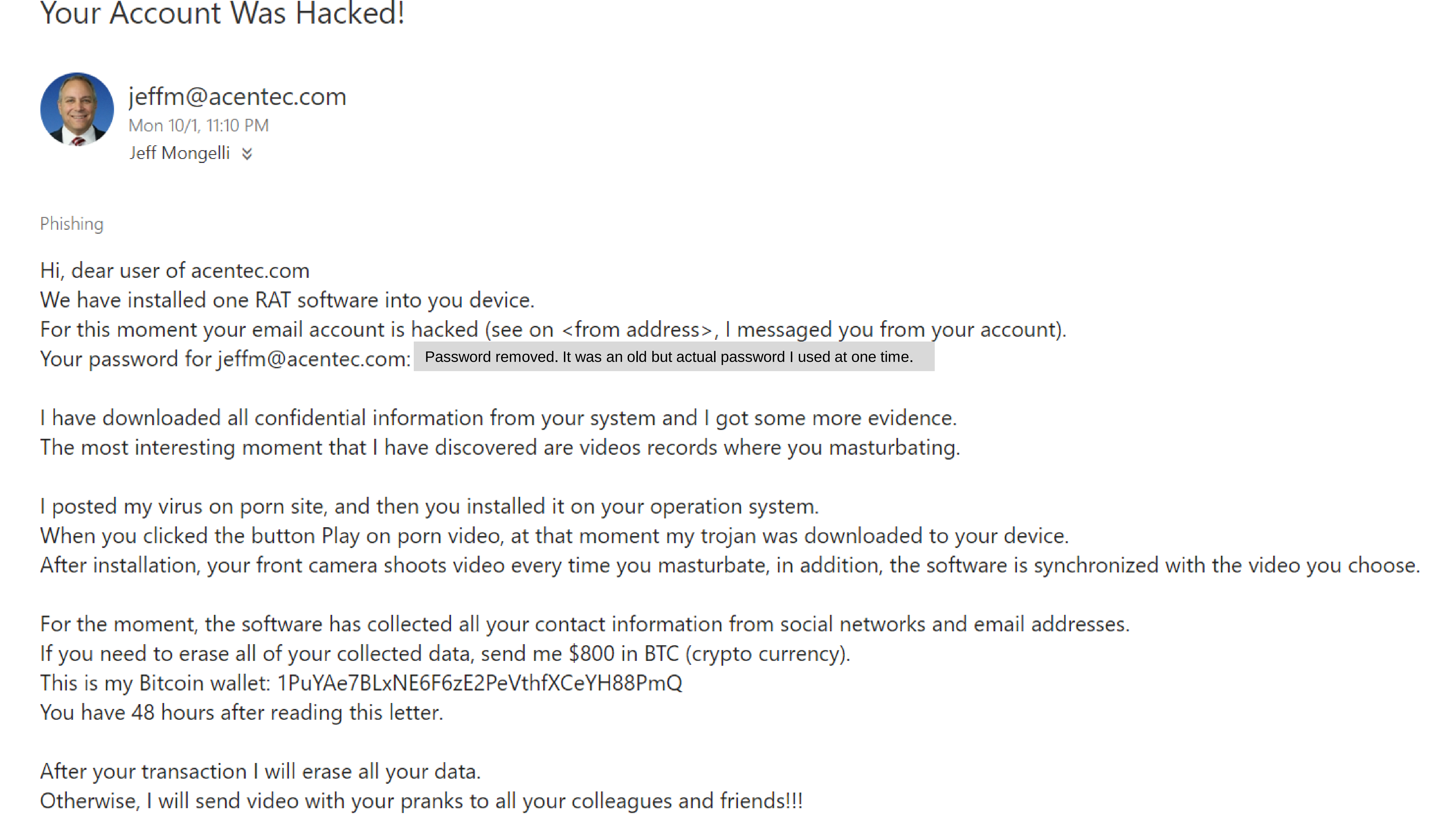
Orthopaedic Surgery-...
96 KB

Hi,

Could you review the attached document. File has been securely scanned and uploaded using Dropbox Business for sharing.

Regards,

[redacted]



Your Account Was Hacked!

jeffm@acentec.com
Mon 10/1, 11:10 PM
Jeff Mongelli

Phishing

Hi, dear user of acentec.com
We have installed one RAT software into you device.
For this moment your email account is hacked (see on <from address>, I messaged you from your account).
Your password for jeffm@acentec.com: Password removed. It was an old but actual password I used at one time.

I have downloaded all confidential information from your system and I got some more evidence.
The most interesting moment that I have discovered are videos records where you masturbating.

I posted my virus on porn site, and then you installed it on your operation system.
When you clicked the button Play on porn video, at that moment my trojan was downloaded to your device.
After installation, your front camera shoots video every time you masturbate, in addition, the software is synchronized with the video you choose.

For the moment, the software has collected all your contact information from social networks and email addresses.
If you need to erase all of your collected data, send me $800 in BTC (crypto currency).
This is my Bitcoin wallet: 1PuYAe7BLxNE6F6zE2PeVthfXCeYH88PmQ
You have 48 hours after reading this letter.

After your transaction I will erase all your data.
Otherwise, I will send video with your pranks to all your colleagues and friends!!!

Reducing your risk

- Don’t take the bait!

CLICK ME!

I Promise

Reducing your risk

- **Passwords**
  - Most popular passwords for years have been password123 and 123456
  - how good are we at protecting our keys to the kingdom?

Reducing your risk

- **Passwords**
  - Biometrics to the rescue, right?

Reducing your risk

- **Passwords**
  - New NIST guidance recommends passphrases

Thisismypasswordandyoucantguessit

Is better than:

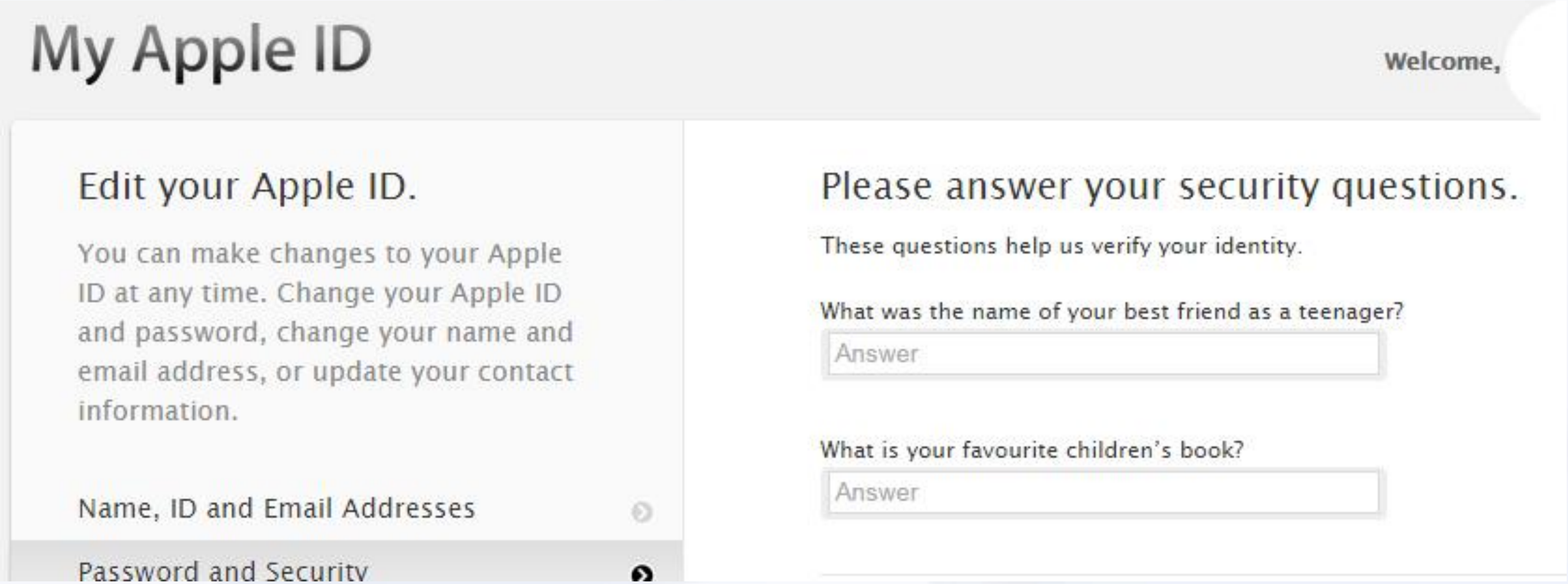
P@55W0rd!

Reducing your risk

- **Passwords**
  - NIST also recommends doing away with regular password changes.
  - WE DISAGREE!

Reducing your risk

- **Passwords**
  - Security questions - lie



My Apple ID

Edit your Apple ID.

You can make changes to your Apple ID at any time. Change your Apple ID and password, change your name and email address, or update your contact information.

Please answer your security questions.

These questions help us verify your identity.

What was the name of your best friend as a teenager?

What is your favourite children's book?

Acentec
Improving Medical Practice Performance®

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

HIPAA® SECURITY SUITE
Your Key to HIPAA Compliance®

Reducing your risk

- **Social Media**
  - Clean up your social media life

Reducing your risk

- **Protect your home network**
  - Your home and your mobile devices are your hospital's Achilles heel.
  - Upgrade your home router

Reducing your risk

- **Protect your facility**
  - Nextgen firewalls – Sophos, Fortinet
    - Web based
    - Update for threats automatically
  - Dark web scanning – ID Agent, Experian

Acentec
Improving Medical Practice Performance®

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

HIPAA® SECURITY SUITE
Your Key to HIPAA Compliance®

Reducing your risk

- **Personal protection**
  - Strengthen (lengthen) your passwords.
  - Get smart about social media.
  - Use a credit/identity protection service – Lifelock, Experian
  - Lock your credit
  - Use complex passwords for financial and shopping sites
  - Use a password manager – Roboform, LastPass

Reducing your risk

- **Sign up for HIPAA Compliance & Security Reminders**

  Pursuant to Section 164.308(a)(5) of the HIPAA Security Rule, the Standard states: Implement a security awareness and training program for all members of its workforce (including management).

  - They're FREE
  - They're weekly
  - They meet HIPAA best practices recommendations
  - https://hipaasecuritysuite.com/hipaa-compliant-security-reminders/

Acentec
Improving Medical Practice Performance®

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

HIPAA® SECURITY SUITE
Your Key to HIPAA Compliance®

Questions?

Acentec
Improving Medical Practice Performance®

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

HIPAA® SECURITY SUITE
Your Key to HIPAA Compliance®

Thank you

Jeff Mongelli

CEO

Acentec, Inc.

HIPAA Compliance
Healthcare IT Management
jeffm@acentec.com
800-970-0402
www.acentec.com

Acentec
Improving Medical Practice Performance®

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

HIPAA® SECURITY SUITE
Your Key to HIPAA Compliance®