Cybersecurity

Defending Your Church from Cybersecurity Threats

Brotherhood Mutual
Matt Cohee, Sr. InfoSec Engineer

BROTHERHOOD MUTUAL®

Today’s Cyber-Agenda

- **Why Cyber Matters to Churches**
- **Security 101** - Best practices
- **Ransomware** - and how to avoid it
- **Insurance** - Cybersecurity coverage & transferring risk
- **Question & Answer**

BROTHERHOOD MUTUAL®

Why should Ministries Care about Cybersecurity?

- Faith & Trust are our ‘stock & trade’
- We are a “sanctuary” for: children, counseling, grief, etc. and this should extend to our protection of private data

- Why churches are a target?
    - Organized Crime simply looks for easy targets
    - Hospitals and Financial institutions are becoming tougher targets
    - Disruptive malware from State-actors is generally indiscriminate
    - Hacktivists – Ideologically targeting

BROTHERHOOD MUTUAL®

Ministries Have What Hackers Want

- Personally Identifiable Information:
  - First and last names
  - Date of birth
  - Age
  - Address
  - Social Security numbers
  - Email address
  - Telephone numbers
  - Credit card numbers
  - Health records
  - Criminal records

BROTHERHOOD MUTUAL®

Keeping Data Safe (standard best practices)

Basic	Advanced
Patching	Know where your (sensitive) data is
2FA (especially VPN)	Password Vault/Manager
Separate Guest Wi-Fi	Encrypt All Laptops
RDP behind VPN	DNS security for your Domain
Managing Credentials	
Governance	Governance

BROTHERHOOD MUTUAL®

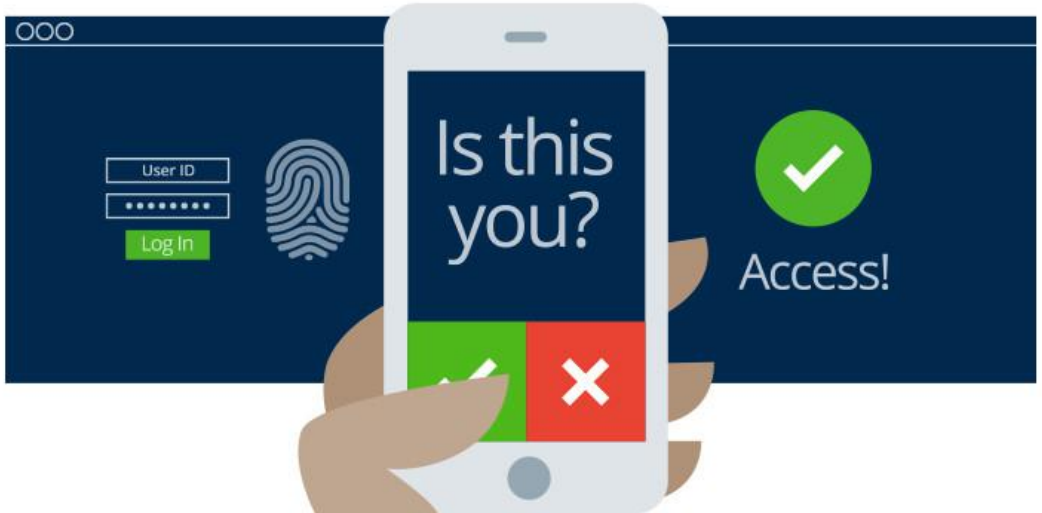
Patching

- Why? – Known vulnerabilities
- Church (file server, email, ChMS, etc)
- Personal (phone, laptop, Acrobat, Java, etc.)
- Bad reasons to not patch
  - I don’t like change
  - My computer will reboot and it takes too long
  - I’m out of space
- Don’t download patches from unfamiliar sites (use auto-update)

BROTHERHOOD MUTUAL®

Multi-Factor Authentication (MFA or 2FA)

- Something you know (password) and something you are/have
- Your banks already require this (and Apple)
- 2nd factor (Email, text msg, biometric, App on phone)
- Recommended for:
  - Any site with info you want to protect (TurboTax)
  - Amazon / Shopping
  - Email
  - VPN
  - All banking

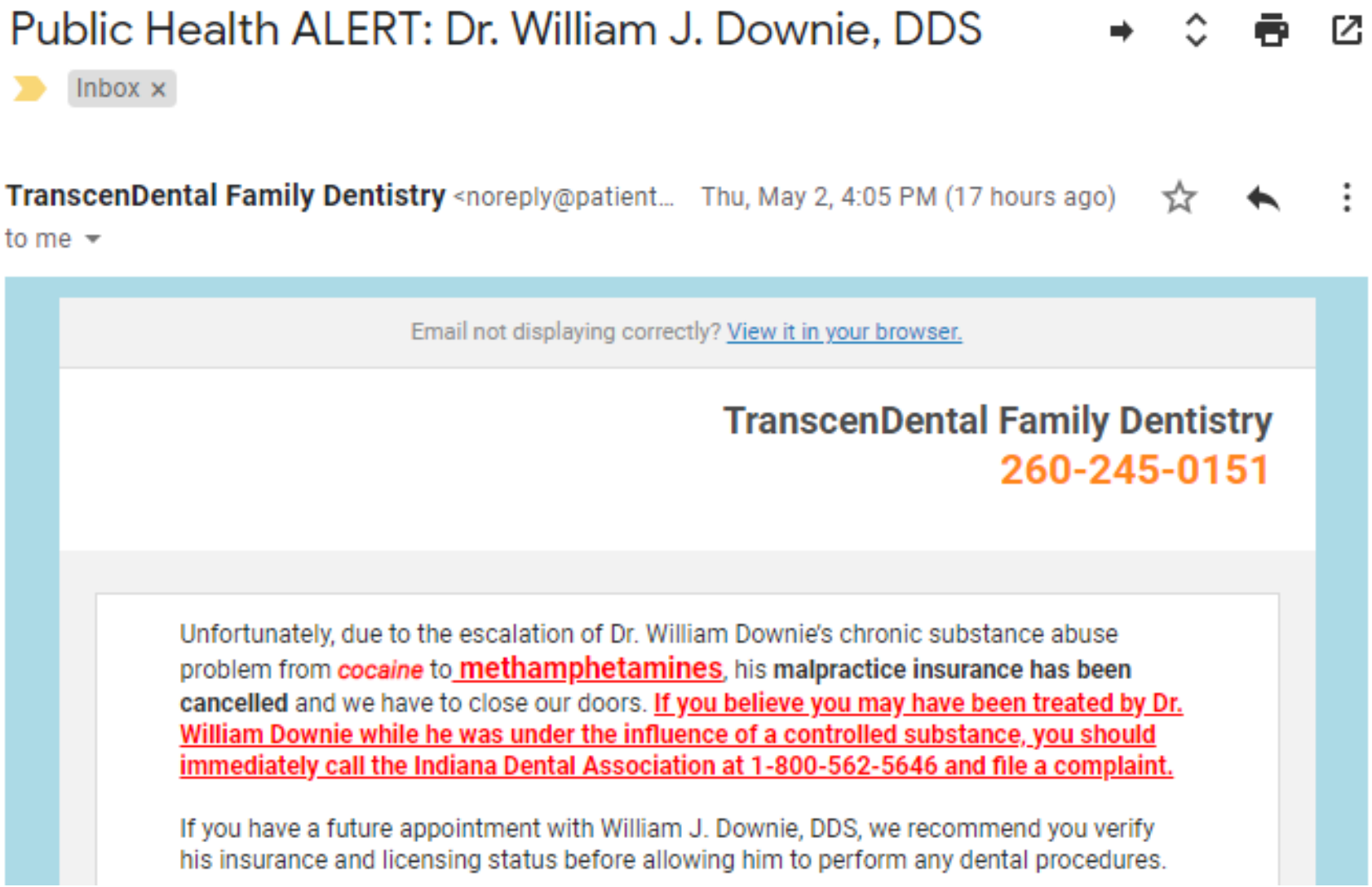


BROTHERHOOD MUTUAL®

Guest Wi-Fi | VPN access | RDP connections

- Guest Wi-Fi should NOT have access to church admin systems
- VPN access to the church network should require MFA
- Church Administration Systems
  - Protected by VPN
  - OR if cloud based, protected by MFA (especially payroll & admin)
- RDP (remote desktop protocol) systems same as ChAdmin

BROTHERHOOD MUTUAL®



Public Health ALERT: Dr. William J. Downie, DDS

Inbox ×

TranscenDental Family Dentistry <noreply@patient… Thu, May 2, 4:05 PM (17 hours ago)

to me

Email not displaying correctly? View it in your browser.

TranscenDental Family Dentistry
260-245-0151

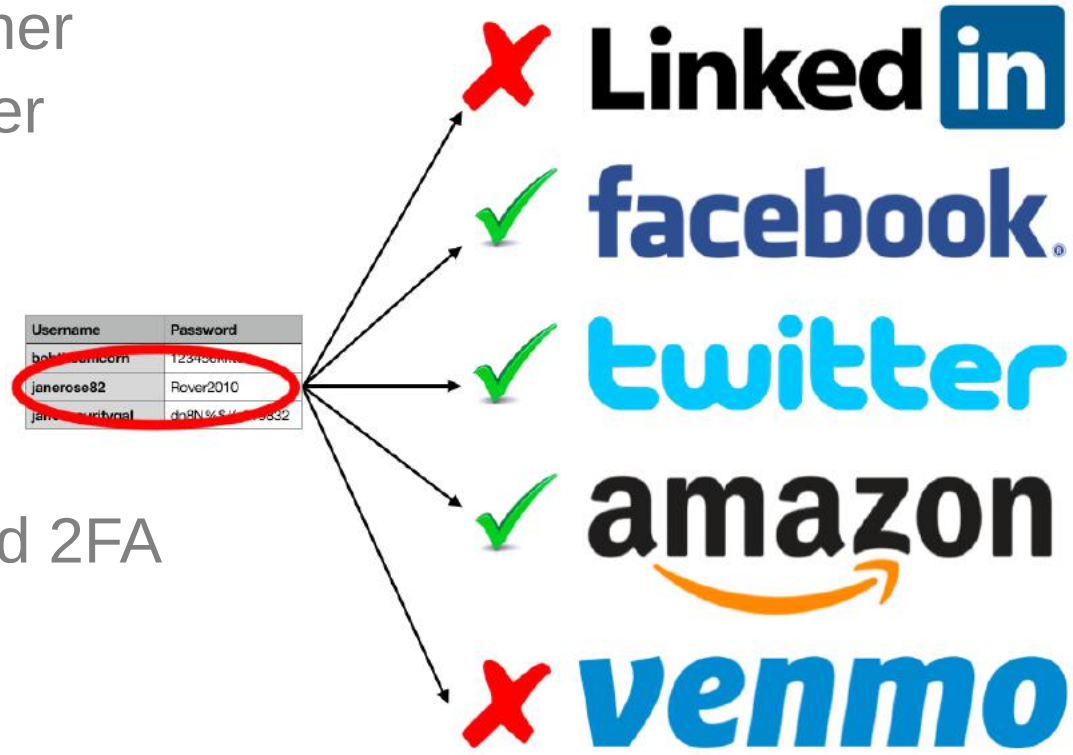
Unfortunately, due to the escalation of Dr. William Downie's chronic substance abuse problem from *cocaine* to **methamphetamines**, his **malpractice insurance has been cancelled** and we have to close our doors. **If you believe you may have been treated by Dr. William Downie while he was under the influence of a controlled substance, you should immediately call the Indiana Dental Association at 1-800-562-5646 and file a complaint.**

If you have a future appointment with William J. Downie, DDS, we recommend you verify his insurance and licensing status before allowing him to perform any dental procedures.

BROTHERHOOD MUTUAL

The Password Problem…Credential Stuffing !

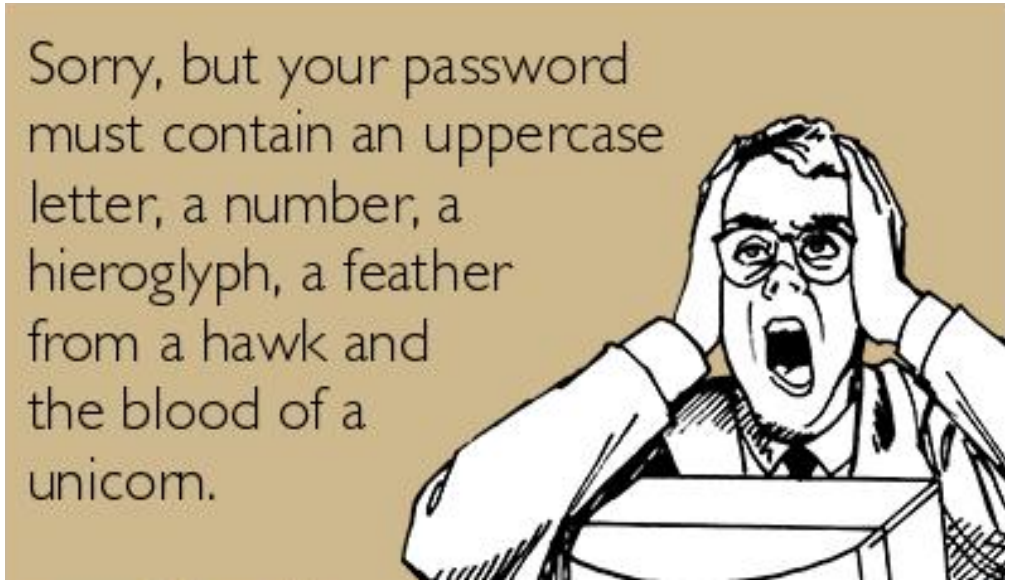
- Use of leaked credentials (usually stolen in a data breach), applied to dozens of other accounts, hoping for Account-Takeover
- Botnets used to distribute attacks
- Credential collection through Trojan Sites, theft on minor site
- Best Defense: Unique passwords and 2FA



BROTHERHOOD MUTUAL

Password Manager

- Why? Credential Theft (Phishing & Password Stuffing)
- Enables - long, complex, and unique/random passwords
- Advantages:
  - Saves time (after setup)
  - Safe/encrypted
  - Backed up to the cloud
  - Sync to all computers and devices
  - Spouse friendly



BROTHERHOOD MUTUAL®

Governance for Cybersecurity

- Why?
  - Align security efforts with ministry goals/values
  - Clarify responsibility and roles
- Who? (roles)
  - CISO or Equivalent (chief information security officer)
  - Steering Committee – provides resource & input
  - The Board – provides accountability
- How? - Risk Management approach (cost/benefit)

BROTHERHOOD MUTUAL®

Key Components of your Cybersecurity Program

- Policies
- Regularly Reviewed and Communicated
- Incident Response Plan
- Disaster Recovery Plan
- Employee Training

BROTHERHOOD MUTUAL®

Ransomware

Ransomware

- Q1 payments - $137k average, $47k median
- 81% threaten to publish stolen data
- 23 days of downtime is average
- 75% - less than 1000 emp. (small/med)
- 90% from Phishing and RDP compromise
- No single industry or sector is targeted
- Good Backups are your best defense

BROTHERHOOD MUTUAL

Source: coveware.com

Ransom vs Extortion

- Ransom - You pay to get something back (to unencrypt)
  - Tech easy to break and you need it to function
- Extortion – You pay to avoid info being released
  - Tech is in our private space (voice, video, email, chat)
  - DDoS – Distributed Denial of Service
  - Recent spam claiming to have video of you

BROTHERHOOD MUTUAL®

Extortion Email

Wed 7/11/2018 8:35 AM

Firstname Lastname <Username@provider.com>

username – password

To username@recipient.com

I know, P@55w0rD , is your password. You don't know me and you are most likely wondering why you are getting this mail, right?

Well, I actually setup a viru5 on the "videos" (adult material) site and you visited this website for fun (you know what I mean). While you were watching video clips, your browser began functioning as a RdP (Remote control Desktop) with a keylogger which gave me access to your display as well as web camera. Right after that, my software obtained every one of your contacts from your Messenger, FB, as well as email.

What exactly did I do?

I created a split-screen video. First part shows the video you were viewing (you've got a fine taste hehe), and 2nd part shows the recording of your web camera.

exactly what should you do?

Well, I believe, $___ is a fair price tag for our little secret. You'll make the payment through Bitcoin (if you do not know this, search "how to buy bitcoin" in Google).

BTC Address: <BTCAddress>
(It is cAsE sensitive, so copy and paste it)

BROTHERHOOD MUTUAL®

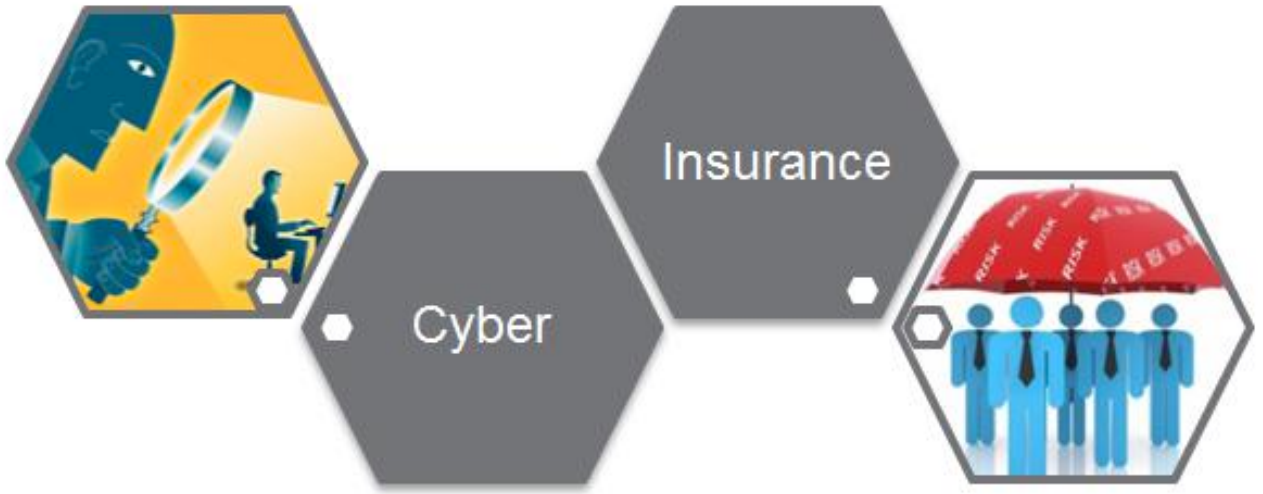
Ransomware Protection

Basic	Advanced
Data Backups	Application Whitelisting
Email Hygiene	Remove Admin Rights (laptops)
Employee training	Air-gap Backup
Web Filtering (OpenDNS)	Backup Laptops
Disaster Recovery planning/testing	Cloud file storage
	Incident Response Plan

BROTHERHOOD MUTUAL®

Cyber Insurance (transferring risk)

- Important part of managing risk
- Ask your agent about...
  - Coverage limitations
  - Liability to others for Cyber Damages
  - Forensics & discovery
  - Breach recovery & rectification
  - Ransomware
  - Vendor Email Compromise (VEC)
  - Voluntary parting
- **FREE** Brotherhood Mutual tools:
  - Legal Assist
  - Resource Library (videos, articles, guidebooks)



BROTHERHOOD MUTUAL®

BROTHERHOOD MUTUAL®

QUESTION AND ANSWER