Carney Forensics

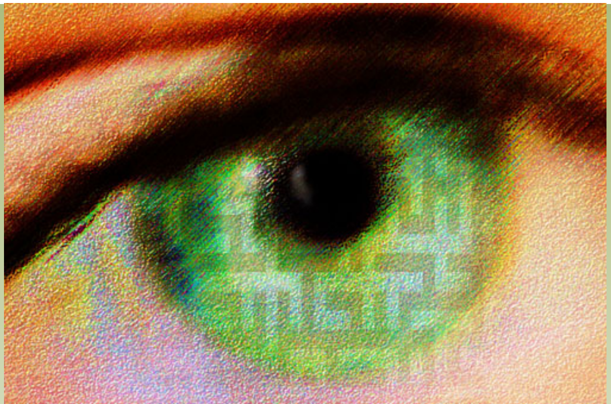
How To Keep Your Documents and Network Secure When Working Remotely

MinnCLE Probate and Trust Law Section Conference

June 8, 2021

John J. Carney, Esq.

Carney Forensics



Security & Legal Ethics

Four Basic ABA Model Rules that Govern

Rule 1.1	**Competence**
Rule 1.4	Communications
Rule 1.6	Duty of **Confidentiality**
Rule 5.1, 5.2, 5.3	Lawyer & Nonlawyer Associations

The **"Big Two"** in Network or Cybersecurity

Begin Your Journey Toward **Competence** to Keep *Office* Data, Documents, and Communication **Confidential**

38 States Have Adopted Revised Rule 1.1

"To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*"

Network Security

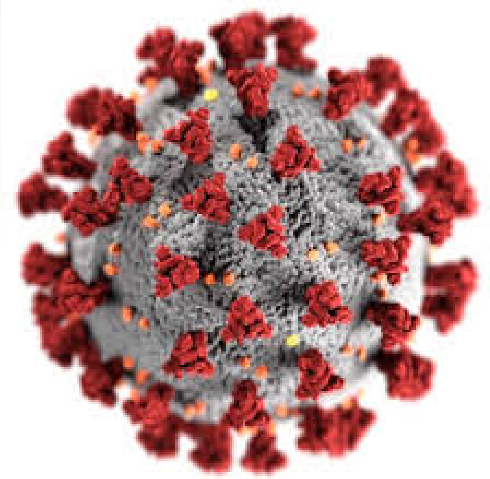
What Are We Worried About?

Data Breaches (ABA: 26% of firms breached)
Viruses and Malware (ABA: 36% attacked with malware)
Privacy Breaches
Theft of IP (Documents)
Ransomware
Spyware
Advanced Exploits
Breaking and Entering
Stolen Workstations

Working Remotely
All the Above!!

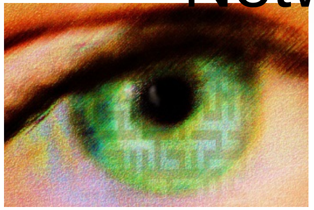
Working Remotely

- Many of Us Will Not Be Returning to the Office after COVID-19
- Or, Maybe We’ll Work from Home a Few Days a Week
- Information Security Risk Working from Home is 3.5 Times the Risk of Working in the Office
- What Will YOU Do?



Working Remotely

- What Will You Do?
  - Protect your Law Firm’s Network, Workstations, and Mobile Devices at Work, Home, and Third Places
- How Will You Do It?
  - Focus on Proactive Steps to Limit Risk of Document Loss and Network Breach
  - Evaluate Solutions for Solo, Small, and Medium Size Law Firms including All the Latest Technology
  - Use Tips Shared Here to Keep Your Documents and Network Secure Working Remotely



Remote Office Router

- What is a Router?
- Router is a Traffic Cop:
  - Between Internet and Workstations
  - Between Server and Workstations
  - Between Workstations in the Law Office

- Most Important Security Device in your Law Office
- and ***Working from Home!!***

Remote Office Router Security

- Security Depends on Frequently Updated Firmware for Life of Router
- Updated Firmware Protects Router Against Exploits, Vulnerabilities, Bugs, etc.
- Firmware Updates Add New Security Features

Remote Office Router Security

- Security Depends on Wise Configuration Choices
- Hackers Commonly Exploit Known Router Defaults
- So, You Must Replace All Router Setting Defaults
  - Use Custom, Strong Router Login Passcode
  - Use Custom, Strong Wi-Fi Network Passcode
- Backup Your Firmware and Router Configuration for Quick Disaster Recovery

Remote Office Router Security

- Prohibit Remote Access to Router for Management
- Turn Off All Remote Access Configuration Settings
- Allow Only *On-site* Access for Router Management and Changing Settings
    - Ethernet only for Router Management
    - No Wi-Fi for Router Management

Remote Network Access?

- Do You Allow Remote Access to Your Law Office?
- You May be Exposing Your Office to Network Vulnerabilities

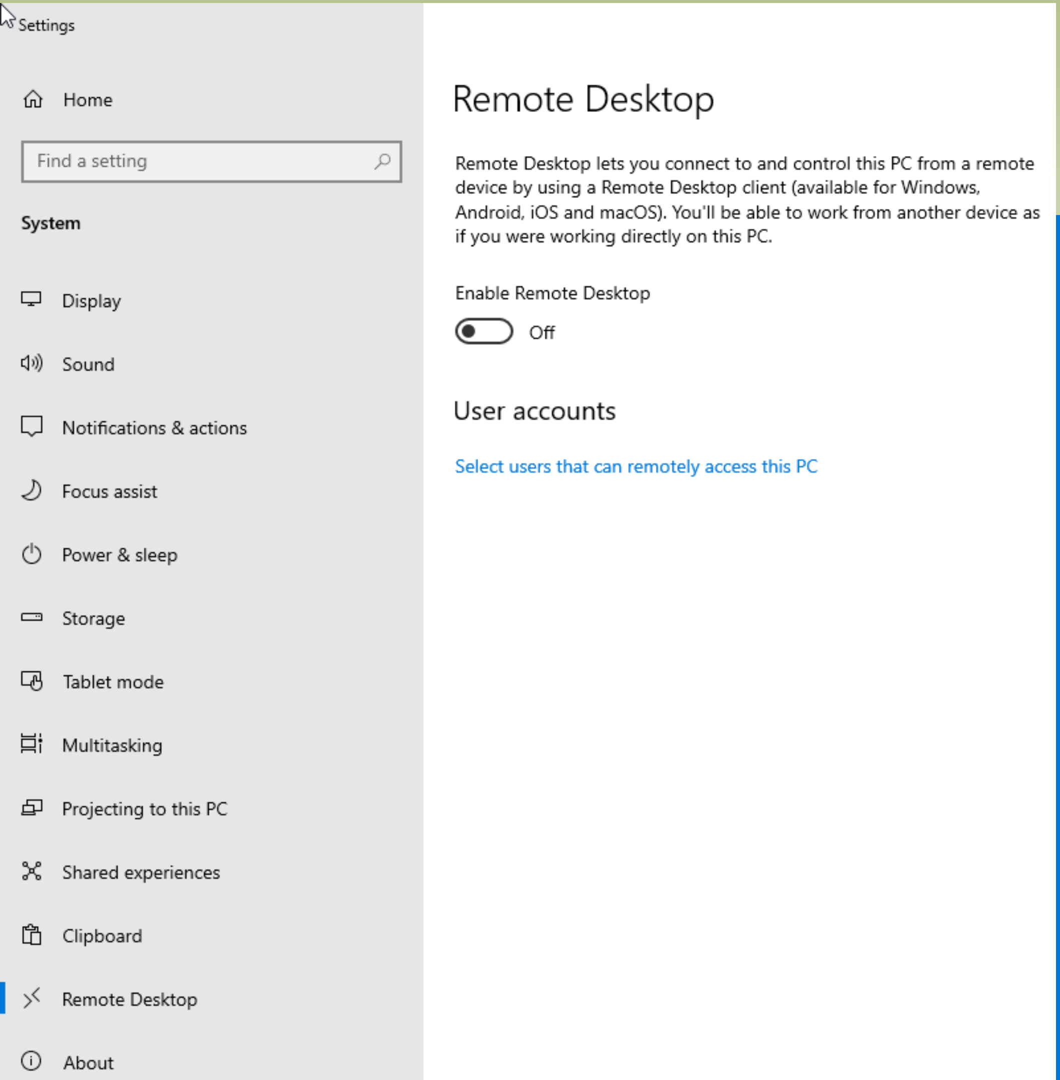
- Prohibit Remote Access to Law Office Router for Router Management and Changing Settings
- Turn Off All Remote Access Configuration Settings
- Allow Only *On-site* Access for Law Office Router Management
  - Ethernet only
  - No Wi-Fi

Remote Desktop Protocol (RDP)

- Allows Control of Remote Windows PC as if You Were Directly Connected to it
- “Remote” into Law Office Computer from Home
- FBI and DHS Warning: Attack Vector for Malware
- Stop Using Microsoft Remote Desktop (RDP)
- Or, Disable RDP When Not Using It

Remote Desktop Protocol (RDP)

- Disable Microsoft Remote Desktop (RDP)



Remote Desktop

Remote Desktop lets you connect to and control this PC from a remote device by using a Remote Desktop client (available for Windows, Android, iOS and macOS). You'll be able to work from another device as if you were working directly on this PC.

Enable Remote Desktop

○ Off

User accounts

Select users that can remotely access this PC

Network Vulnerability Scans

- Proactively Test Your Network for Vulnerabilities
- Scan Your Network for Holes Like a Hacker Would
- It’s Called “Intrusion Detection” or “Ethical Hacking”
- Best Done Professionally
- But Qualys Has a Free Cloud-based Network Scanner
- And Qualys Has a Free Web App Scanner for Testing Your Law Office Web Site

Update Operating Systems

- What Kind of Workstations Using Remotely?
  - Windows?
  - Mac?
- Update Expired Windows Desktops and Laptops
  - **NO** Windows 7, Windows Vista, Windows XP
  - Windows 10 ($199 MSRP for “Pro”)
  - Windows 8 Still Okay

Update Operating Systems

- Time Is of the Essence When Patching Exploits and System Vulnerabilities
- Users Must Update Immediately to New Patched OS Versions
- Patch Tuesday Is Time for “Windows Update” for Windows, Office, and Everything Microsoft

- MacOS X App Store Supports OS “Updates”
- Also MacPaw CleanMyMac X

- IObit’s Driver Booster

Update Applications

- Windows Apps, Browsers, Utilities, and BIOS Must Be Patched Frequently & Systematically
- Ninite Pro Patches Apps, Browsers, Utilities, .NET, Java, and Other Windows Software
- Ninite Pro Has Dashboards for Windows Patches for All Workstation Configs in Your Law Office
- IObit's Windows Software Updater
- MacOS X App Store Supports Apps "Updates"
- Also MacPaw CleanMyMac X

Ninite

Install and Update All Your Programs at Once

Malware Protection

- Detect and Remove Viruses, Exploits, Spyware
- Protect Against Zero Day Exploits with Behavioral, and Heuristic Methods
- Protect Against Drive-by Download Attacks for Safe Web Surfing

- Be Alert for Hidden or Disguised Hardware USB Keyloggers

Windows Malware Protection

- Microsoft Windows Defender Detects Virus, Spyware, Malware. Enable It Today!

- Malwarebytes for Teams
- Powerful, easy-to-use cybersecurity solution for small businesses that provides advanced protection against malware, ransomware, and hackers

MALWAREBYTES
FOR TEAMS

Apple Mac Malware Protection

- MacPaw CleanMyMac X

MacPaw

- Antivirus Zap
- Malwarebytes for Teams

Ransomware Protection

- Ransomware is Malicious, Cryptovirology Software
- Hackers Demand Ransom Payments from Users
- Threaten to Publish User’s Data to Third Parties
- Threaten to Withhold Decryption Keys which Block User’s Access to their Documents and Data

- Attack Vectors: Email Phishing, Remote Desktop,
  Lack of Software Updates

ZONEALARM
By Check Point

MALWAREBYTES
FOR TEAMS

Password Managers

- Create Strong, Complex Passwords Automatically
- Log You into Sites and Apps Automatically
- Have Password Health Scorecard for Improvement
- Highlight Password Reuse for Correction
- Automatic Notification of Compromised Passwords
- Safely Share Your Passwords with Team
- Password Changer Wizard for Easy Fixes
- Consider Third Party Options:
  - Dashlane
  - 1Password
  - LastPass
  - eWallet
  - iCloud Keychain

Two-Factor Authentication (2FA)

- It’s a 2nd, Time-based Password for Secure Access to Web Accounts and Mobile Apps
- It’s Something You “Know”, “Possess”, or “Are”
  - “Know” Your Passwords, Pass Phrases, and PINs
  - “Possess” Your Smart Phone for Confirmation from Authenticator Apps
  - “Possess” Your YubiKey (USB Security Key) for Convenient Authentication
  - You “Are” Your Biometric Fingerprint, Face Scan, Retina Scan

Two-Factor Authentication (2FA)

- Google says 2FA Blocks Attacks
  - “We found that an SMS code sent to a recovery phone number helped block 100% of automated bots, 96% of bulk phishing attacks, and 76% of targeted attacks. On-device prompts, a more secure replacement for SMS, helped prevent 100% of automated bots, 99% of bulk phishing attacks and 90% of targeted attacks.”
- Microsoft says 2FA Blocks 99% of Attacks
- You Need 2FA More When Working Remotely
  - Office 365, Gmail, Dropbox, Clio, MyCase, etc.

    - Load Google Authenticator on Your Smart Phone
    - Bring Your YubiKey (USB Security Key) Home

VPN @ Work from Home

- Virtual Private Network (VPN) Service Provides Secure Access to Online Apps on Internet
  - Email – Office365, Gmail, etc.
  - Cloud – Google Docs, Dropbox, Practice Mgt.
- Encryption Connection Protects from Improperly Configured Router
- Use VPN Service on Computers @ WFH
  - Laptops, Netbooks, Desktops, also Tablets, Phones
- NordVPN Protects Six Devices at the Same Time Anywhere Inexpensively

NordVPN®

VPN @ Third Places

- Insecure Public Wi-Fi is Everywhere
  - Coffee Shops, Restaurants, Airports, Hotels
  - Conferences, Law Firms, Skyway
- Always Use VPN Service on Laptops When Insecure Public Wi-Fi is Your Only Option
- Use VPN Service on Smart Phones and Tablets for Public Wi-Fi Protection
- Pay for Your VPN. No-charge VPN Products Are Often Decoys Provided by Hackers to Steal or Leak Your Data

NordVPN®

Privileged Access Management

- Privileged Admin Accounts on Computers and Online Accounts Have Elevated Permissions to Critical and Confidential Information & Resources
- Privileged Admin Accounts are High Value Targets for Cyber Criminals and Present Serious Risks
- 44% of Data Breaches Last Year Involve Privileged Admin Accounts

- So, Work Logged Into a User Account, Not an Admin Account (Windows, Mac, Online Apps, etc.)

Mandatory Backups

- Backups are Solution to Data Losses, Breaches, and Harmful Exploits of All Types

- Loose Files and Folder Backup Tools Abound
  - 2BrightSparks SynchBack SE (Try SynchBackFree)
- Disaster Recovery Solution for Quick Drive Restores
  - We Use Paragon Hard Disk Manager ***Advanced***
- You Must Regularly and Systematically Test Backup Reliability by Simulating Data Loss Emergencies

SyncBackFree

Everyday Backup

2BrightSparks Pte Ltd © 2013

www.2BrightSparks.com

POWER WITH EASE - INDISPENSABLE UTILITY SOFTWARE

Paragon SOFTWARE GROUP

Mandatory Backups

It’s Your Responsibility Now Working from Home

- Windows 10 “File History”
- Windows “Backup and Restore”
- macOS “Time Machine”

Cloud Backups are Convenient

- CrashPlan for Small Business
- Microsoft OneDrive
- Google Drive
- Dropbox

CRASHPLAN

Storage Encryption

- Full Disk Encryption Protects Against Data Breach
- Invaluable When Disk Drives are Lost, Stolen, Crash
- Safe Harbor in Many Data Breach Statutes
  - HIPAA and Some State Government Privacy Laws
- Encrypt Computer Disk Drives and Backups
- Microsoft BitLocker is Bundled into Windows
- WinMagic SecureDoc Encryption Solution
  - Provides Security Key Management
- Encrypt Removable Drives Like Flash Drives with Password to Protect Documents
  - Microsoft BitLocker-To-Go
  - Easy to Use and No Charge

Reduce the Attack Surface

- Remove Password Hints from User Login Screen
- Power Off Workstations at Night and Weekends
- Use Ethernet Switches to Disconnect Running Workstations from Networks
- Locate Router in Locked Machine Room or Closet
- Take Drives Offline and Protect in Office Safe
- Take Drives Off-Site and Protect in Safe Deposit Box with Systematic Rotation
- Enforce Retention Policy and Continuously Wipe Sensitive Client Data

Zoom Best Practices

- Configuring Zoom Defaults
  - Waiting Rooms Allow Screening Participants
  - No Participant Entry before Host
  - Disable Screen Sharing as Default
- Using Zoom
  - Use Passwords in Invitations
  - Don’t Use Personal ID in Invitations
  - Host Enable Screen Sharing Privilege Cautiously!!
- Zoom Software Updates a MUST!
  - Every Patch Tuesday?
  - Ninite Pro Supports Zoom Updates

Social Engineering Scams

- Be Alert for Personalized, Targeted Spear Phishing Attacks in Web Mail or E-mail Apps
- Clickjacking Attacks that Trick You into Clicking on a Harmful Link or Attachment
- You Must Train and Test People to Recognize Clickjacking Attacks
- Free Offers for Testing Tools and Simulations

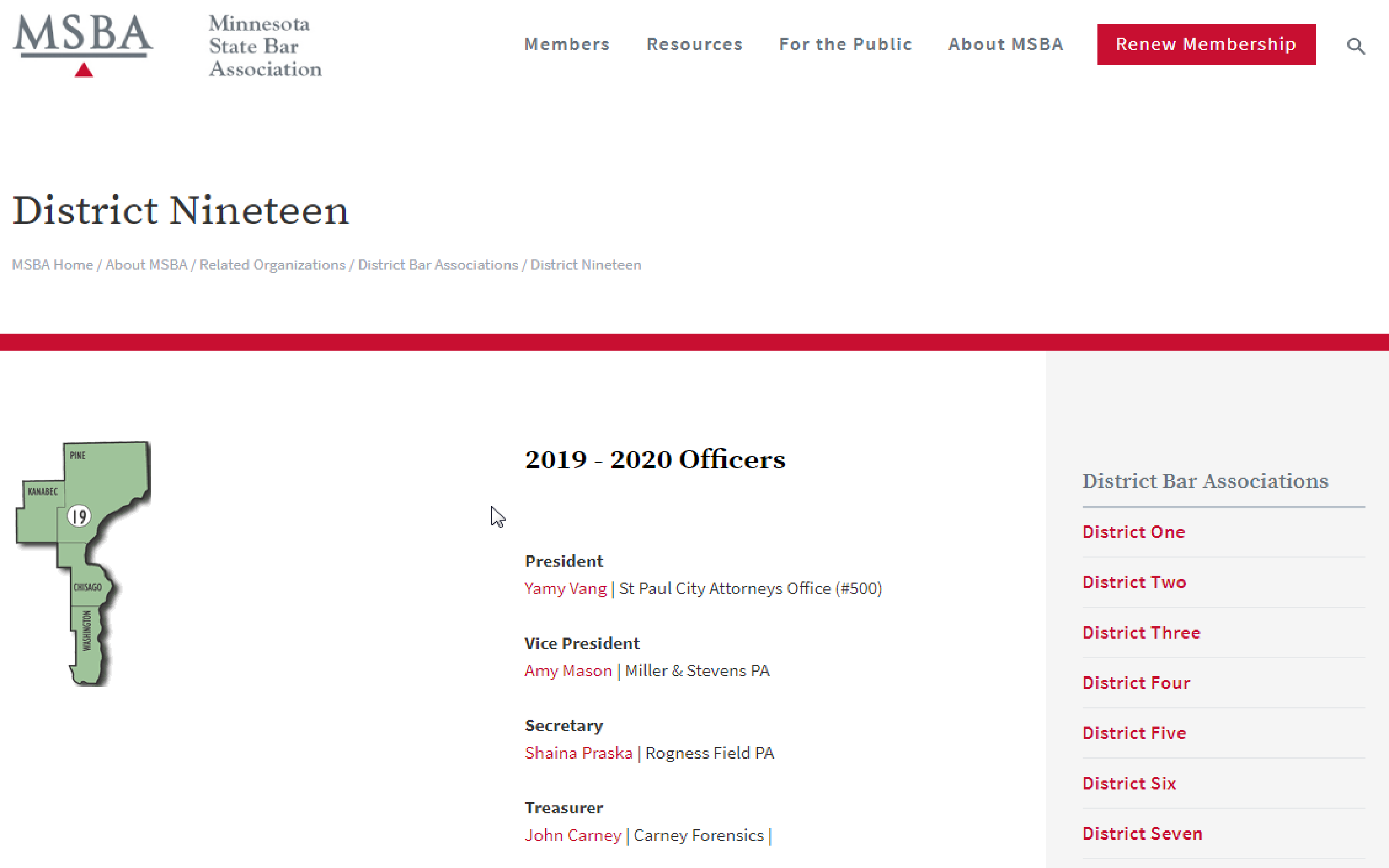
PHISHME

gophish

KnowBe4

Human error. Conquered.

Social Engineering Scams



District Nineteen

MSBA Home / About MSBA / Related Organizations / District Bar Associations / District Nineteen

2019 - 2020 Officers

President
Yamy Vang | St Paul City Attorneys Office (#500)

Vice President
Amy Mason | Miller & Stevens PA

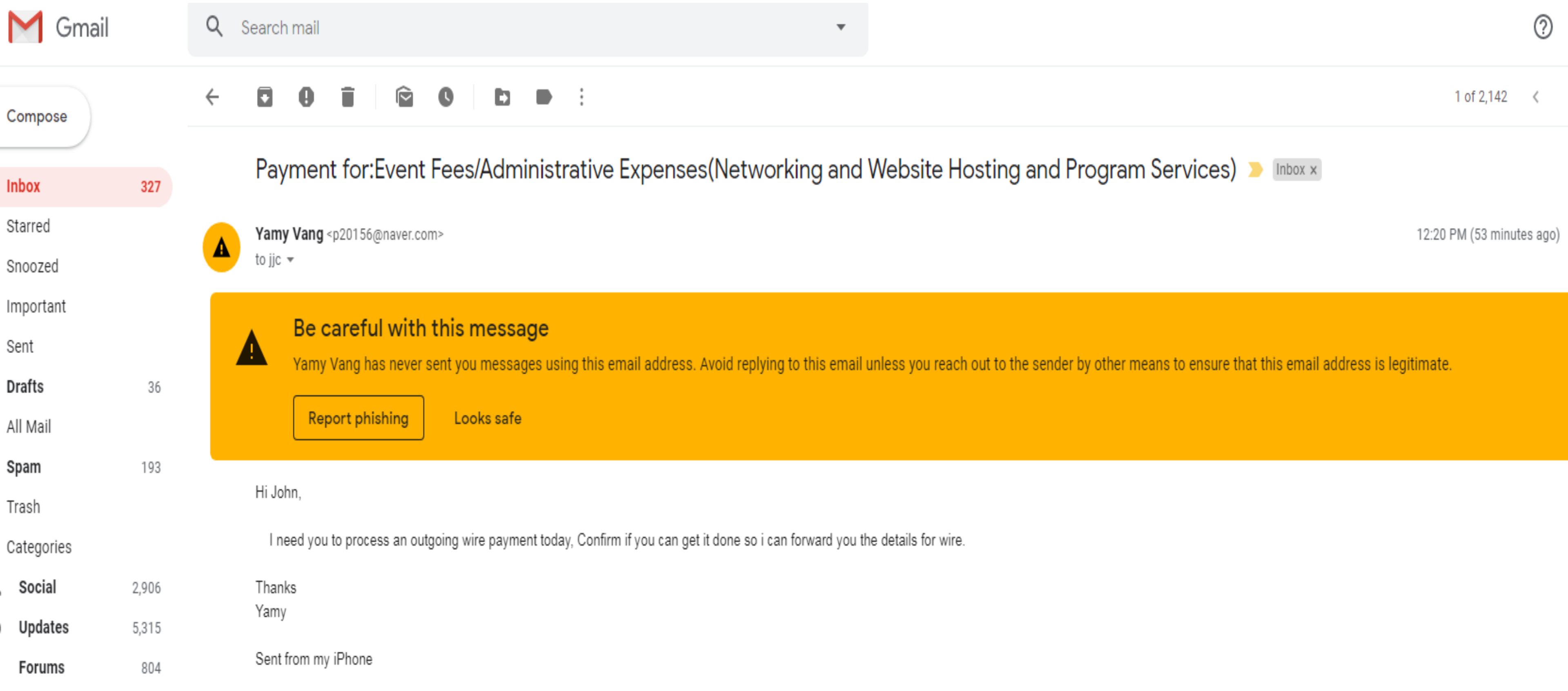
Secretary
Shaina Praska | Rogness Field PA

Treasurer
John Carney | Carney Forensics |

District Bar Associations

- District One
- District Two
- District Three
- District Four
- District Five
- District Six
- District Seven

Social Engineering Scam #1



Payment for:Event Fees/Administrative Expenses(Networking and Website Hosting and Program Services)

Yamy Vang <p20156@naver.com>

to jjc

12:20 PM (53 minutes ago)

Be careful with this message

Yamy Vang has never sent you messages using this email address. Avoid replying to this email unless you reach out to the sender by other means to ensure that this email address is legitimate.

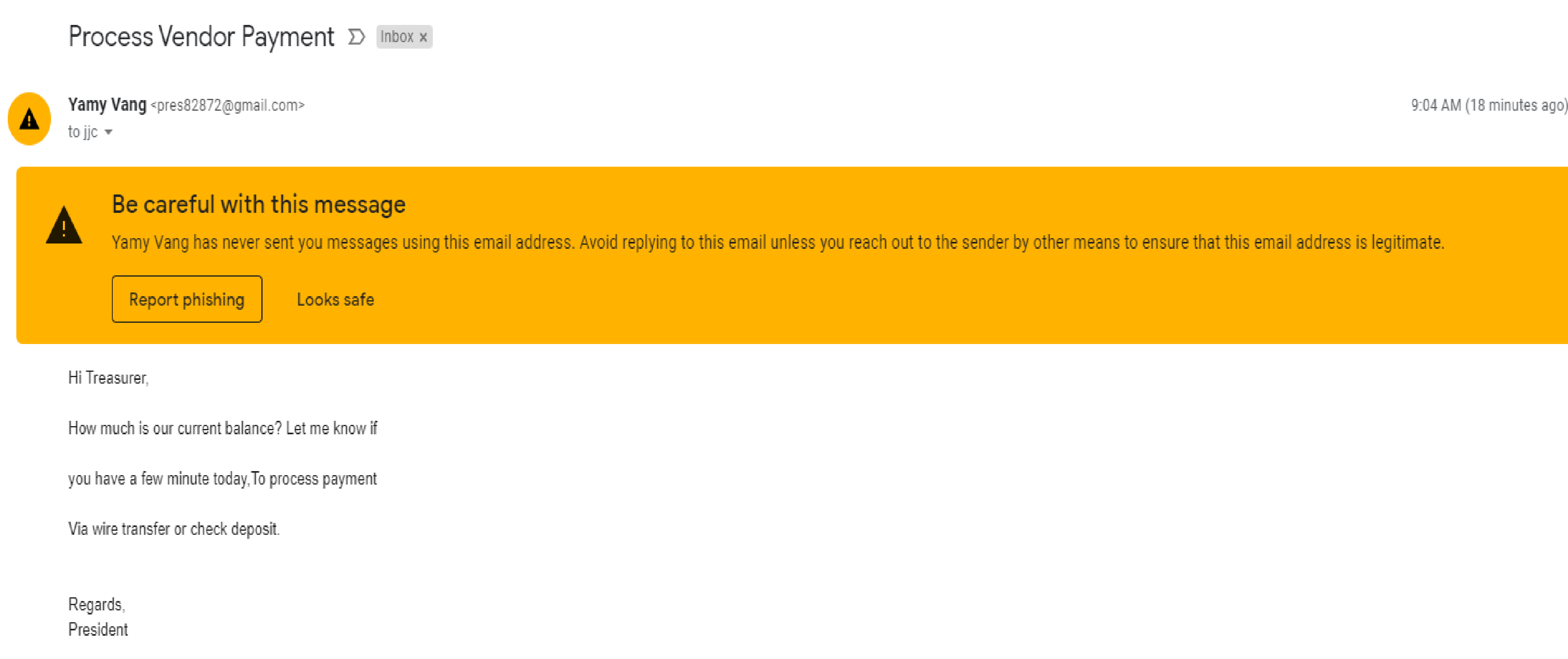
Hi John,

I need you to process an outgoing wire payment today, Confirm if you can get it done so i can forward you the details for wire.

Thanks
Yamy

Sent from my iPhone

Social Engineering Scam #2



Process Vendor Payment

Yamy Vang <pres82872@gmail.com>
to jjc

9:04 AM (18 minutes ago)

Be careful with this message

Yamy Vang has never sent you messages using this email address. Avoid replying to this email unless you reach out to the sender by other means to ensure that this email address is legitimate.

Hi Treasurer,

How much is our current balance? Let me know if

you have a few minute today,To process payment

Via wire transfer or check deposit.

Regards,
President

Questions & Answers

Carney Forensics

"Digital Evidence is Everywhere"

Cell Phones / Smart Phones

Smart Tablets

Computer Forensics

GPS Devices

Social Media / Email

Sign up for our Newsletter!!

www.carneyforensics.com

Carney Forensics