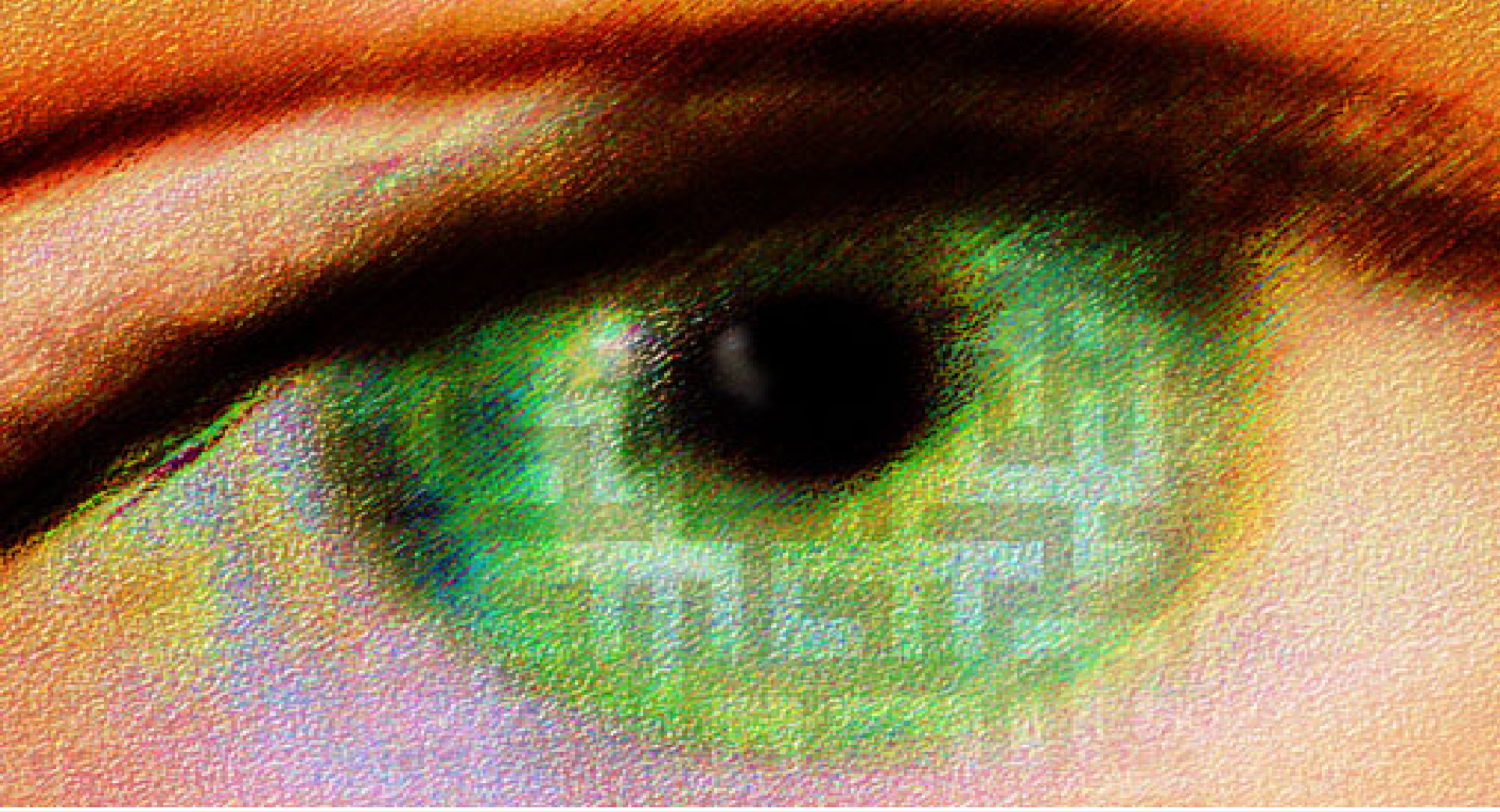


Carney Forensics

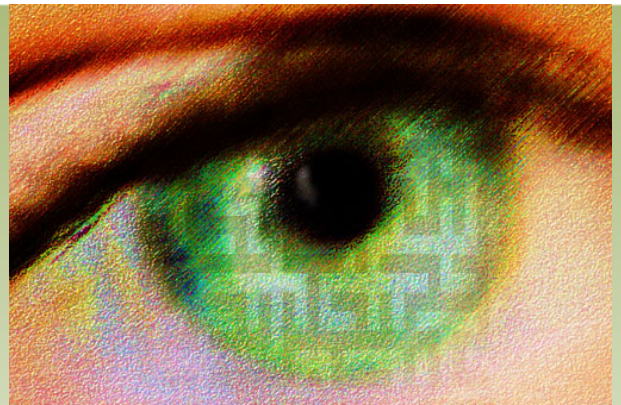
How To Keep A Network Safe At Little To No Cost

Hennepin County Law Library

March 19, 2021

John J. Carney, Esq.

Carney Forensics



Cybersecurity & Legal Ethics

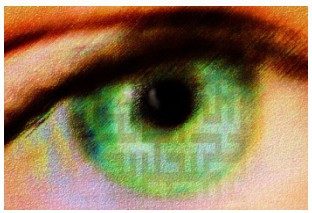
Four Basic ABA Model Rules that Govern

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 Cybersecurity

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

38 States Have Adopted Revised Rule 1.1



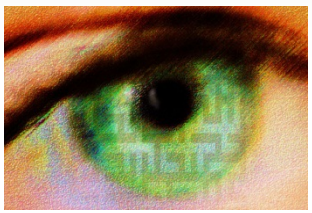
"To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*"

Network Cybersecurity

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
Ransomware
Spyware
Advanced Exploits
Breaking and Entering
Stolen Workstations

Working from Home
All the Above!!



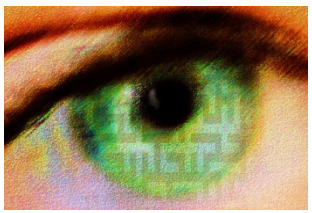
Law Office Router

- 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!!***

Law Office Router Security

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

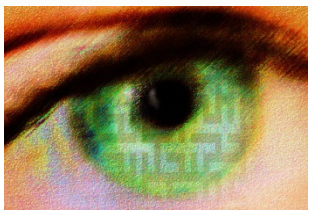


Law Office Router Security

- 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

Law Office Router Security

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



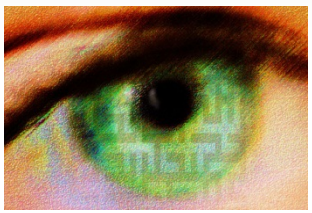
Password Managers

- 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

Update Operating Systems

- What Kind of Law Office Workstations?
  - 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

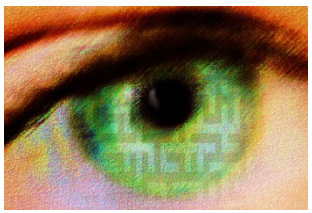


Update Operating Systems

- 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

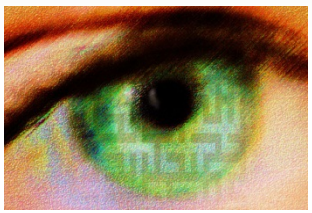
- IObit’s Driver Booster



Microsoft Patch Tuesday

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

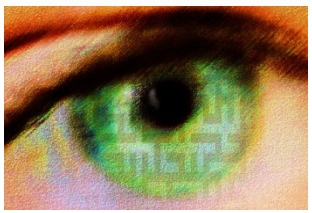
MALWAREBYTES
FOR TEAMS

Apple Mac Malware Protection

- MacPaw CleanMyMac X

- Antivirus Zap

- Malwarebytes for Teams



Ransomware Protection

- Ransomware is Malicious, Cryptovirology Software that Threatens to Publish Victim's Data or Perpetually Block Access Unless a Ransom is Paid
- Attack Vectors: Email Phishing, Remote Desktop, Lack of Software Updates
- Malwarebytes for Teams
- ZoneAlarm Anti-Ransomware

ZONEALARM By Check Point

MALWAREBYTES FOR TEAMS

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

MSBA Minnesota State Bar Association

Members Resources For the Public About MSBA Renew Membership

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

Gmail

Search mail

Compose

Inbox 327
Starred
Snoozed
Important
Sent
Drafts 36
All Mail
Spam 193
Trash
Categories
Social 2,906
Updates 5,315
Forums 804

1 of 2,142

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

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.

Report phishing Looks safe

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 Inbox x

Yamy Vang <pres82872@gmail.com> 9:04 AM (18 minutes ago)
to jjc

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.

Report phishing Looks safe

Hi Treasurer,

How much is our current balance? Let me know if

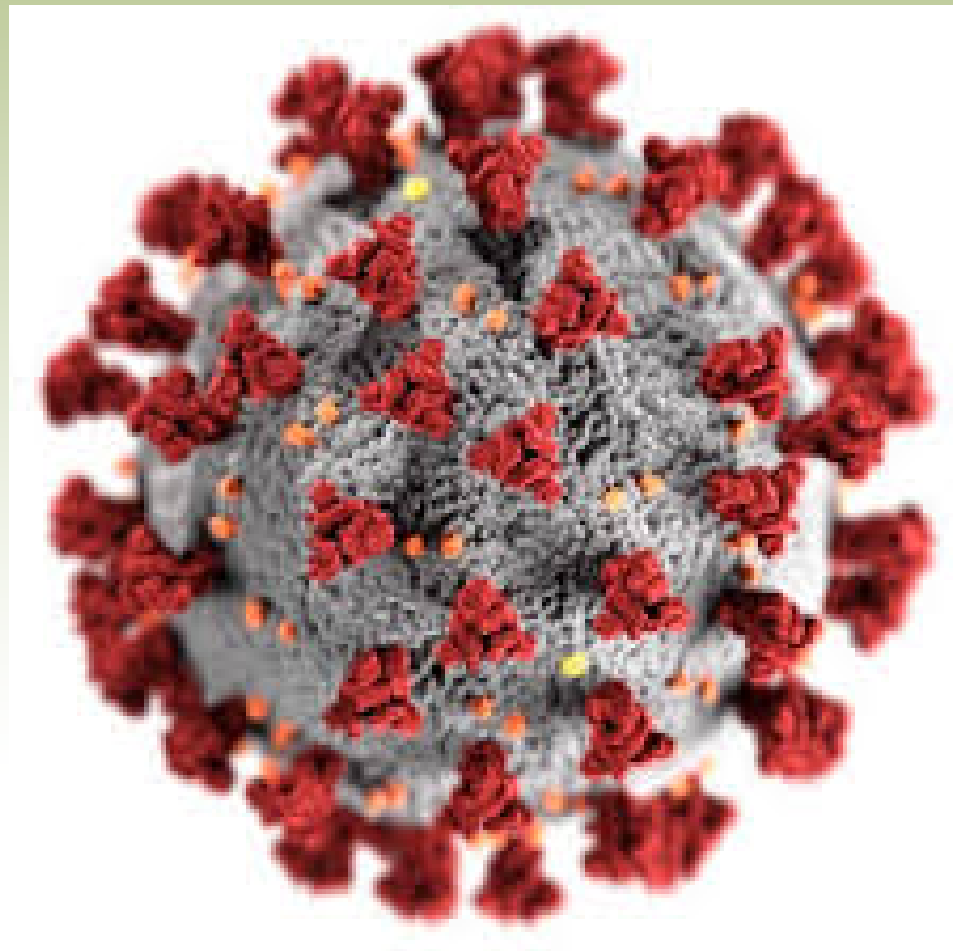
you have a few minute today,To process payment

Via wire transfer or check deposit.

Regards,
President

Working from Home (WFH)

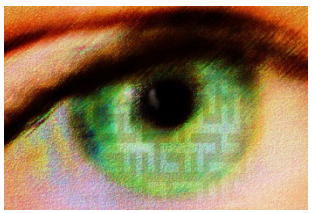
- Information Security Risk WFH is 3.5 times the risk of working in the Office
- What Will YOU Do?



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 Router for Management
- Turn Off All Remote Access Configuration Settings
- Allow Only *On-site* Access for Router Mgt.
    - Ethernet only for Router Management
    - No Wi-Fi for Router Management

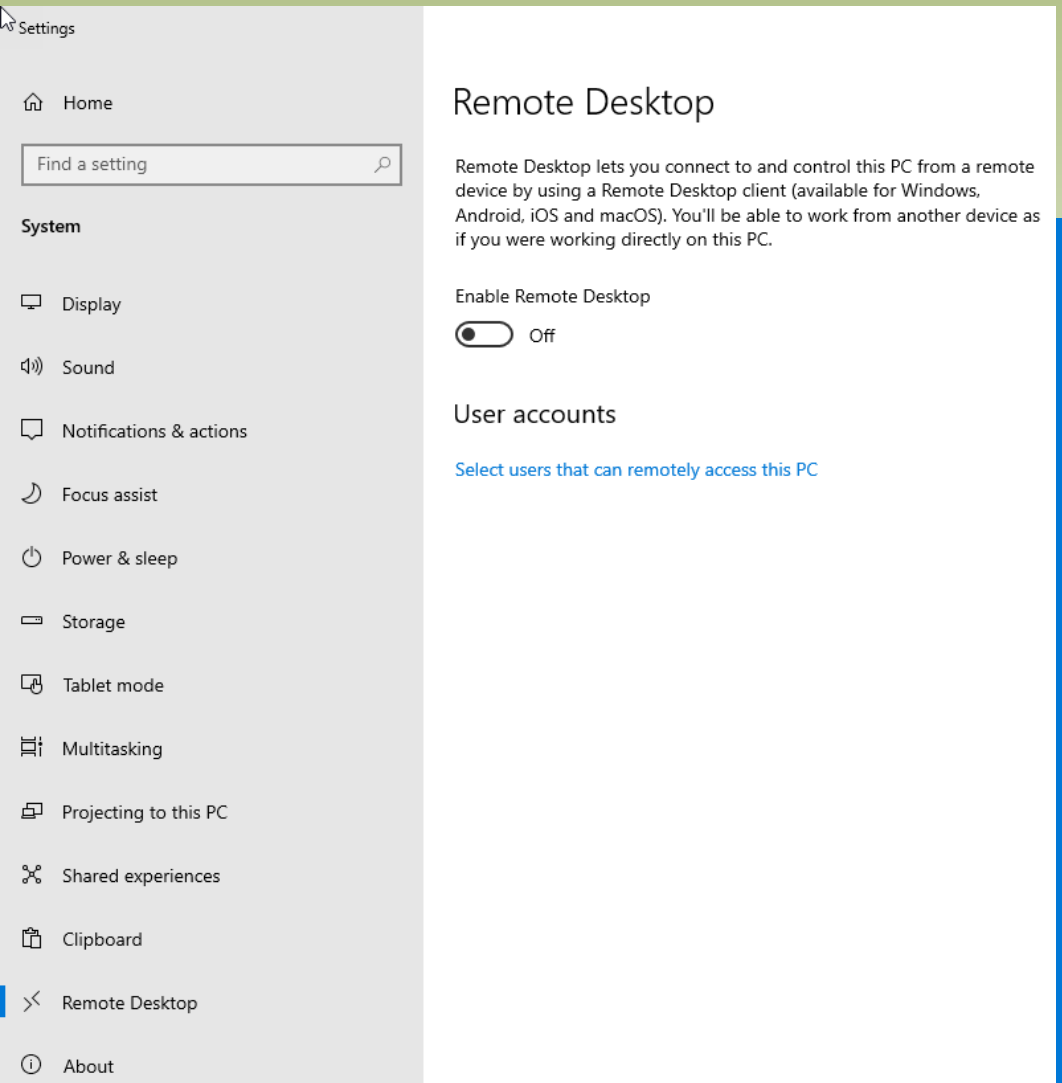


Remote Desktop Protocol (RDP)

- 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)



VPN @ Work from Home

- Virtual Private Network (VPN) Service Provides Secure Access to Email, Cloud, Online Apps
- Protection from Improperly Configured Router
- Use VPN Service on all Computers @ WFH
  - Laptops, Netbooks, Desktops, Tablets, Phones
- NordVPN Protects Six Devices at the Same Time Anywhere Inexpensively

NordVPN®

Two-Factor Authentication (2FA)

- It’s a 2nd, Time-based Password for Secure Access to Web Accounts and Mobile Apps
- Google says 2FA Blocks 100% of Hacks
- Microsoft says 2FA Blocks 99% of Hacks
- You Need It Even More @ WFH
  - Office 365
  - Dropbox
  - Clio, MyCase, CosmoLex, Smokeball, etc.
- Load Google Authenticator on Your Smart Phone
- Bring Your YubiKey (USB Security Key) Home

Mandatory Backups

It's Your Responsibility Now @ WFH

- Windows 10 "File History"
- Windows "Backup and Restore"
- macOS Time Machine

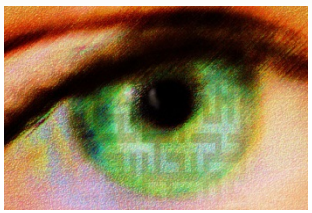
- Regularly Test Your Backups
- Simulate Data Loss Emergency to Discover Failure

- Cloud Backups are Convenient
  - CrashPlan for Small Business
  - Microsoft OneDrive
  - Google Drive
  - Dropbox

CRASHPLAN

Zoom Best Practices

- Configuring Zoom
  - Waiting Rooms Allow Screening Attendees
  - No Attendee Entry before Host
  - Disable Screen Sharing
- Using Zoom
  - Use Passwords in Invitations
  - Don’t Use Personal ID in Invitations
  - Impart Share Screen Privilege Cautiously!!
- Zoom Software Updates a MUST!
  - Every Patch Tuesday?
  - Ninite Pro Supports Zoom Updates



zoom

Reduce the Attack Surface

- 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 the Office Safe
- Take Drives Off-Site and Protect in the Safe Deposit Box with Systematic Rotation
- Enforce Retention Policy and Continuously Delete and Wipe Sensitive Client Data

Questions & Answers

Carney Forensics

"Digital Evidence is Everywhere"

Cell Phones / Smart Phones

Smart Tablets

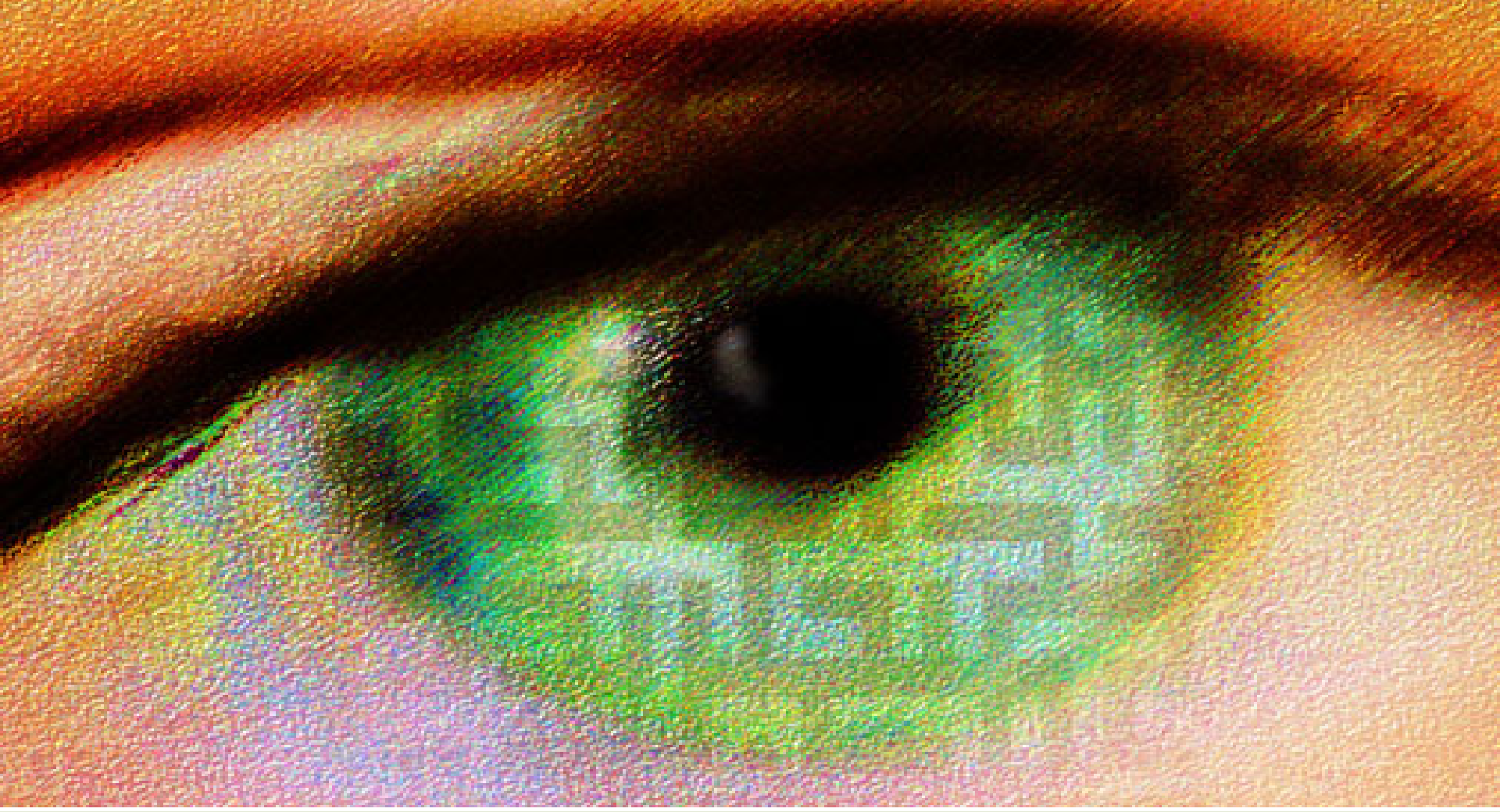
Computer Forensics

GPS Devices

Social Media / Email

Sign up for our Newsletter!!

www.carneyforensics.com



Carney Forensics