Carney Forensics

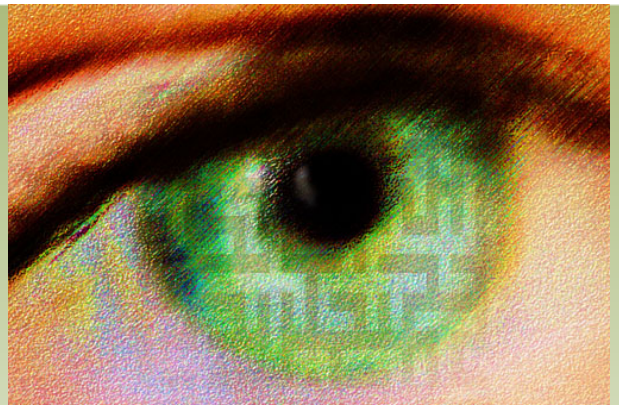
How to Keep a Network Safe at Little to No Cost

Minnesota CLE: Paralegal Program

September 18, 2018

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**

31 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*"

Law Office Cybersecurity

What Are We Worried About?

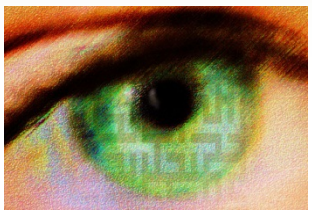
Data Breaches
Privacy Breaches
Theft of IP
Viruses and Malware
Ransomware
Spyware
Advanced Exploits
Breaking and Entering
Stolen Workstations

Scope: Office Workstations

- What Kind of Law Office Workstations?
  - Microsoft Windows Desktops and Laptops
  - Windows 7, Windows 8, Windows 10
  - **NO** Windows XP, Windows 2000, Windows NT

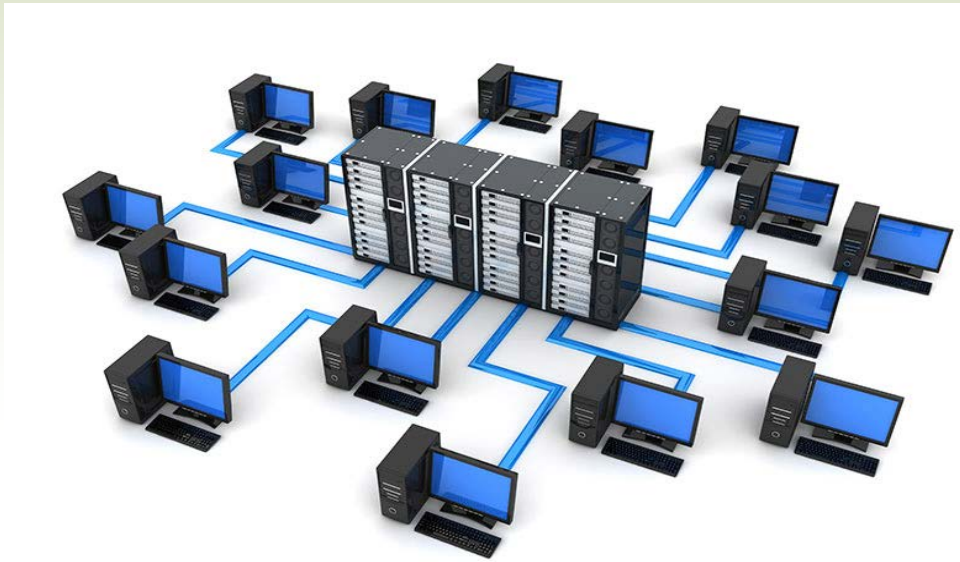
  - Mac OS X iMacs and MacBooks
  - Netbooks like Chromebooks, Dell, HP, Lenovo

- Out of Scope Workstations
  - Linux
  - Android Tablets and iPads



Scope: Office Networks

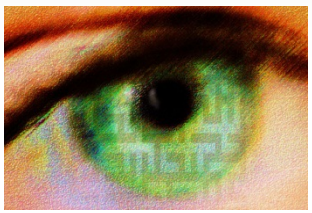
- What Kind of Law Office Networks?
  - Stand Alone Workstations Each with Cloud Access
  - LAN with P2P Connections between Workstations
  - LAN with NAS Device Serving Workstations
    - Storage (Files, Folders, Documents, etc.)
  - LAN with Servers Serving Workstations
    - Storage (Files, Folders, Documents, etc.)
    - Databases
    - Applications



Scope: Office Routers

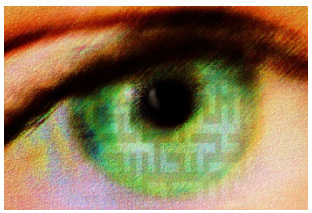
- What is a Router?
- Router is a Traffic Cop:
  - Between Internet and Workstations
  - Between NAS and Workstations
  - Between Server and Workstations
  - Between Workstations in the Office

- Most Important Security Device in a Law Office



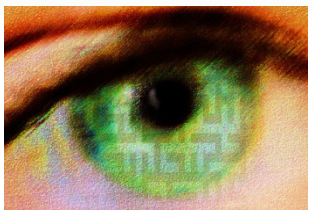
Office Router Security

- Security Depends on Frequently Patched Firmware for Life of Router
- Patched Firmware Protects Router Against Exploits, Vulnerabilities, Bugs
- Firmware Upgrades Add New Security Features
- You Must Choose between Proprietary vs. Open Source Firmware Options
- Popular Open Source Options Include DD-WRT and Tomato
- FlashRouters Offers Routers, Firmware Flashing, Configuration, Support, and Documentation



Office Router Security

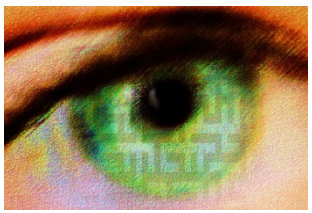
- Security Depends on Wise Configuration Choices
- Hackers Commonly Exploit Known Router Defaults
- So, You Must Replace All Defaults with Custom Values
- Use Custom, Strong Access Passcodes
- Use Custom, Strong WPA2 Encryption Passcodes
- Backup Your Firmware and Router Configurations for Quick Disaster Recovery



Remote Network Access?

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

- Stop Using LogMeIn and GoToMyPC Remotely
- Stop Using Microsoft Remote Desktop (RDP)
- Restrict TeamViewer to Only Troubleshooting Sessions with Trusted Vendors & Off-site Support
- Turn Off All Remote Access Configuration Settings
- Prohibit Remote Access to Router for Management
- Allow Only Onsite Wired Router Access for Mgt.
  - No Router Mgt. from Wi-Fi
  - No Router Mgt. while Offsite

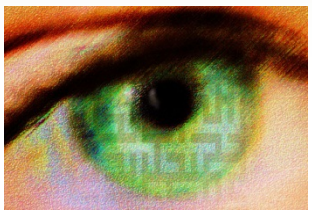


Network Vulnerability Scans

- Test for Network Vulnerabilities Proactively
- Scan Your Network for Holes Like a Hacker Would
- It's Called "Intrusion Detection" or "Ethical Hacking"
- Best Done Professionally
- But If You're Adventurous and Geeky, Qualys Has a Free Cloud-based Network Scanner
- Qualys also Has a Free Web App Scanner for Your Law Office Web Site

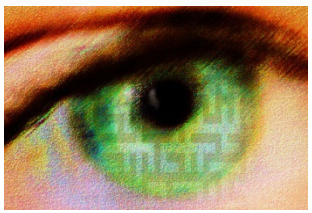
VPN Everywhere

- Virtual Private Network (VPN) Service Provides Access to Secure, Encrypted Network
- Solves Unsecured Wi-Fi Access Point Connection Problem
- Use VPN Service on Laptops and Netbooks When Public Wi-Fi Your Only Option
- NordVPN Protects Six Devices at Same Time Anywhere & Inexpensively
- Office Router Should Be One of Your Six VPN-Protected Devices



Two-Factor Authentication

- It’s a Second, 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



Password Managers

- Creates Strong, Complex Passwords Automatically
- Logs You into Sites and Apps Automatically
- Has Password Health Scorecard for Improvement
- Highlights 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
    - LastPass
    - 1Password
    - eWallet

Patch Operating Systems

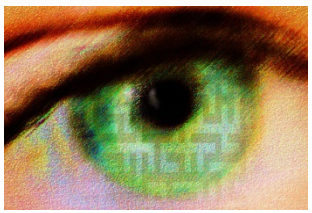
- Time Is of the Essence When Patching Exploits and System Vulnerabilities
- Users Must Upgrade Immediately to New Patched OS Versions
- Patch Tuesday Is Time for “Windows Update” for Windows, Office, and Everything Microsoft

- MacOS X App Store Supports OS “Updates” When Released

Patch Applications

- Windows Apps, Browsers, Utilities, Drivers, 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 and for All Workstation Configs in Your Law Office

- MacOS X App Store Supports Apps “Updates” When Released



Ninite

Install and Update All Your Programs at Once

Malware Protection

- Be Alert for Hidden or Disguised Hardware USB Keyloggers
- Detect and Remove Viruses, Exploits, Spyware, and Keyloggers
- Protect Against Zero Day Exploits with Behavioral, Heuristic, and AI Methods
- Protect Against Drive-by Download Attacks for Safe Web Surfing

Malware Protection

- FortiClient Has a Free Malware Scanner

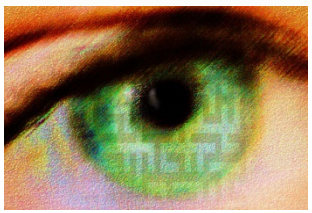
- Microsoft Windows Defender Detects Virus, Spyware, Malware and Ships with Windows

- Malwarebytes Has a Scanner and a Behavioral Exploits Solution

- Webroot Secure Anywhere Has a Behavioral Exploits Solution

Ransomware Protection

- Ransomware is Malicious, Cryptovirology Software that Threatens to Publish Victim's Data or Perpetually Block Access Unless a Ransom is Paid
- CyberReason RansomFree is a Best-in-Class Ransomware Solution
- Malwarebytes Has a Ransomware Solution



Malwarebytes
ANTI-RANSOMWARE
BETA

Rootkit Protection

- Detect and Remove Rootkits, Clandestine Computer Software
- Designed to Provide Privileged Access to a Computer While Actively Hiding Its Presence
- Symantec's Norton Power Eraser Has a Free, Aggressive Rootkit Scan by Default
- Malwarebytes Has an Anti-Rootkit Solution

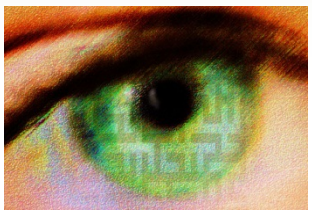
Norton Power Eraser

MALWAREBYTES
CUSTOM ROOTKIT SCAN

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
- PhishMe, Gophish, and KnowBe4 Offer Free Simulated Testing Tools

PHISHME

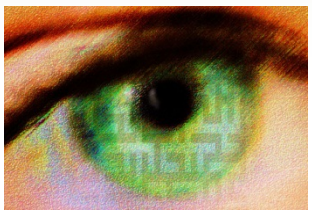


KnowBe4
Human error. Conquered.

gophish

Mandatory Backups

- Backups are Solution to Data Losses and Harmful Exploits of All Types
- Loose Files and Folder Backup Tools Abound
  - 2BrightSparks SynchBack SE (Try SynchBackFree)
- Disaster Recovery Backups for Quick Drive Restore
  - We Use Paragon Hard Disk Manager *Advanced*
- Cloud Backup Tools Abound
  - CrashPlan for Small Business is Excellent
- You Must Regularly and Systematically Test Backup Reliability by Simulating Data Loss Emergencies



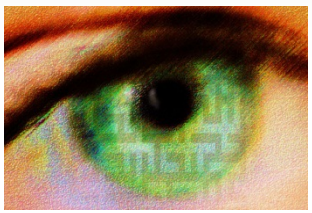
Storage Encryption

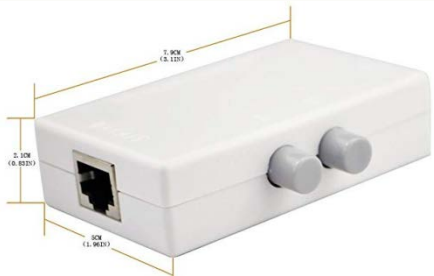
- Full Disk Encryption (FDE) Protects Against Data Loss If and When Drives Go Missing or Crash
- It's a Safe Harbor in Many Data Breach Statutes
  - HIPAA, Some U.S. State Governments
- Encrypt Operating Drives and Backup Drives
- Encrypt Removable Drives Including USB Flash
- WinMagic SecureDoc Encryption Solution for Windows and MacOS X Computers
- Provides Security Key Management w/ Multi-Factor Authentication (Smart Card, Biometric, etc.)

WinMagic SecureDoc

Reduce the Attack Surface

- Work Daily from User Accounts and Restrict Privileged Admin Accounts in Law Office
- 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 Into the Office Safe
- Take Drives Off-Site and Into Safe Deposit Box with Systematic Rotation
- Enforce Retention Policy and Continuously Delete and Wipe Sensitive Client Data





Consult Check List for Tips

How to Keep a Network Safe at Little to No Cost

Protect Your Office from:
Data Breaches, Hackers, Spyware, and More!
for Paralegals

Check List

John J. Carney, Esq.
Carney Forensics
www.carneyforensics.com

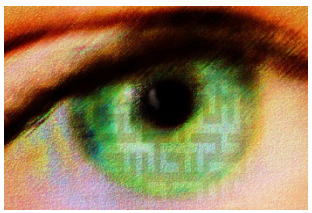


TABLE OF CONTENTS

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