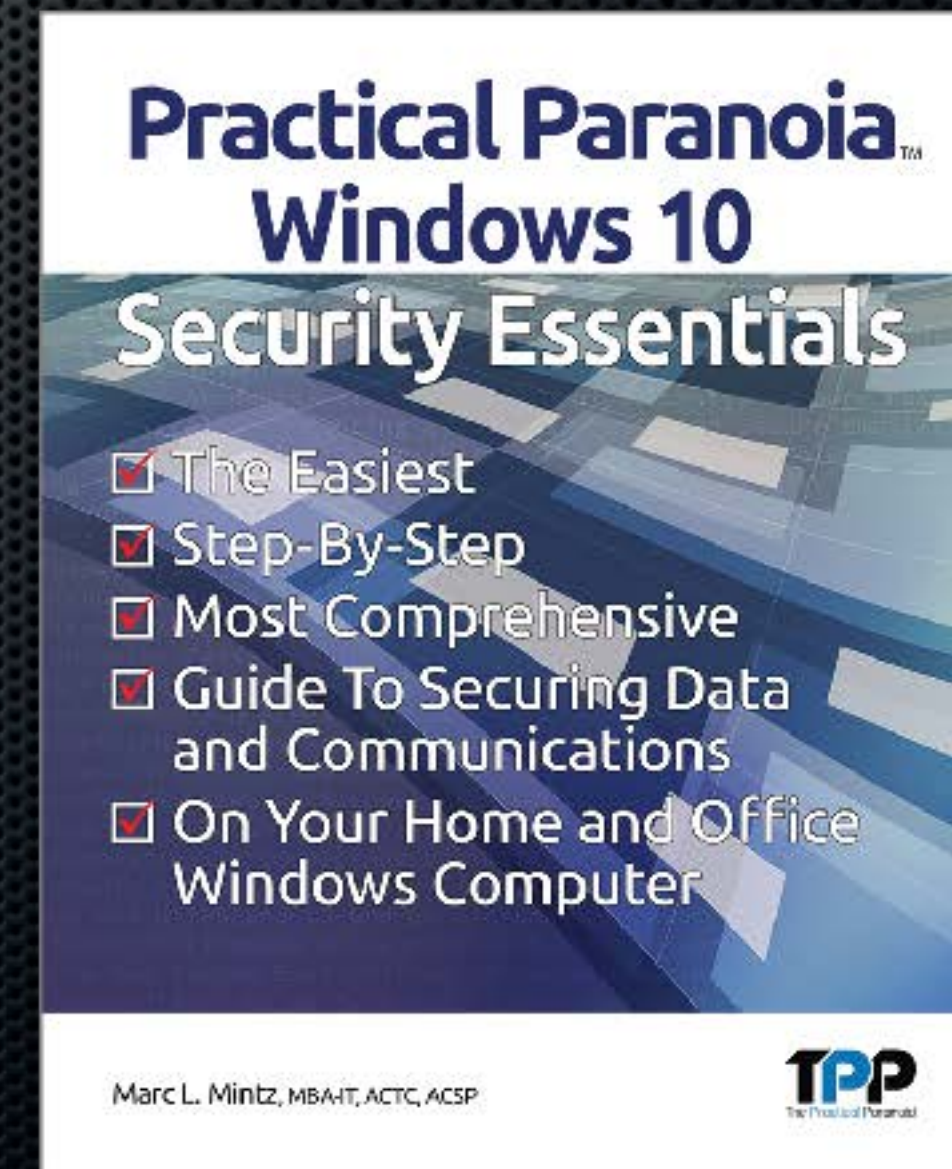
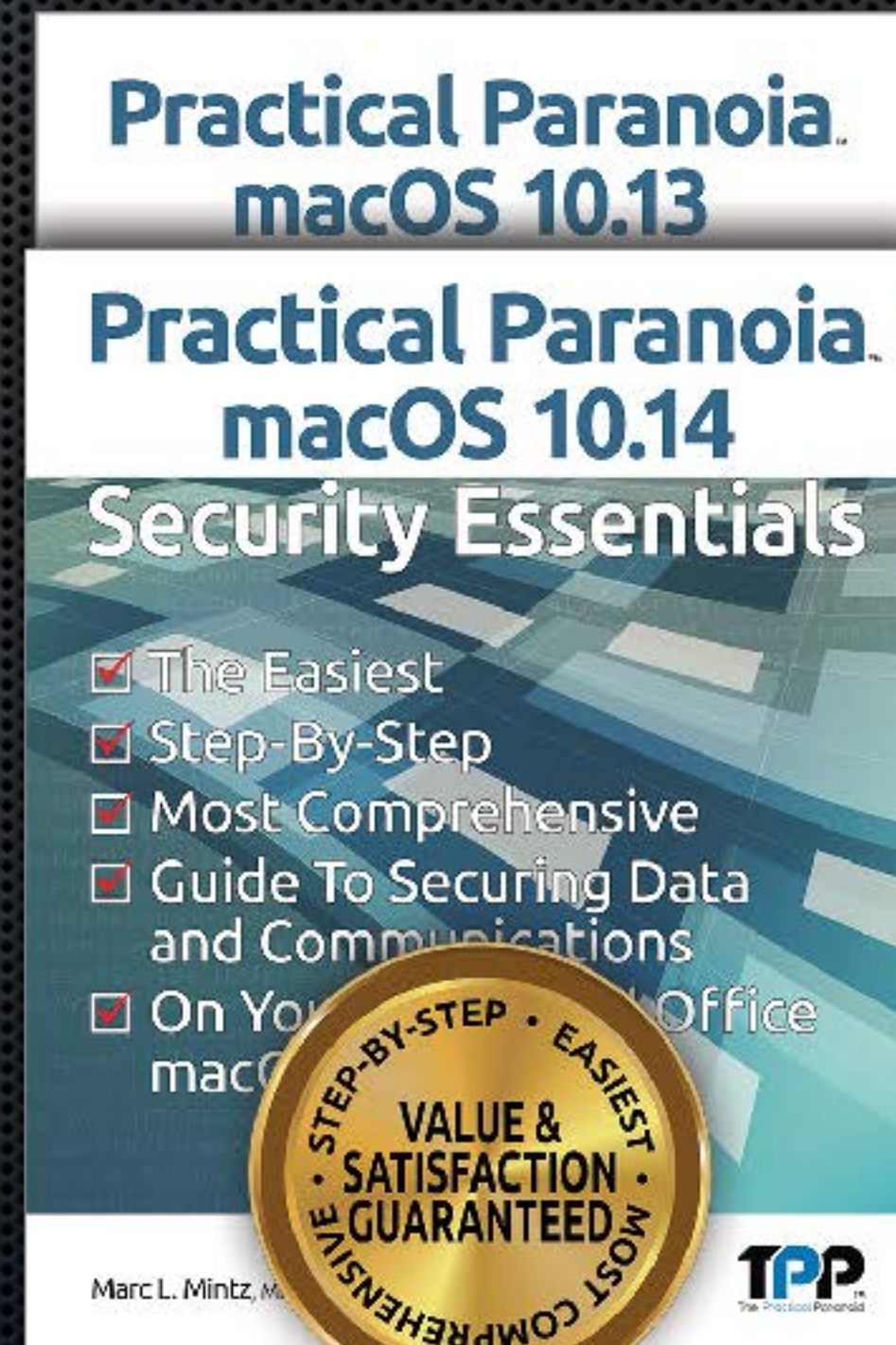
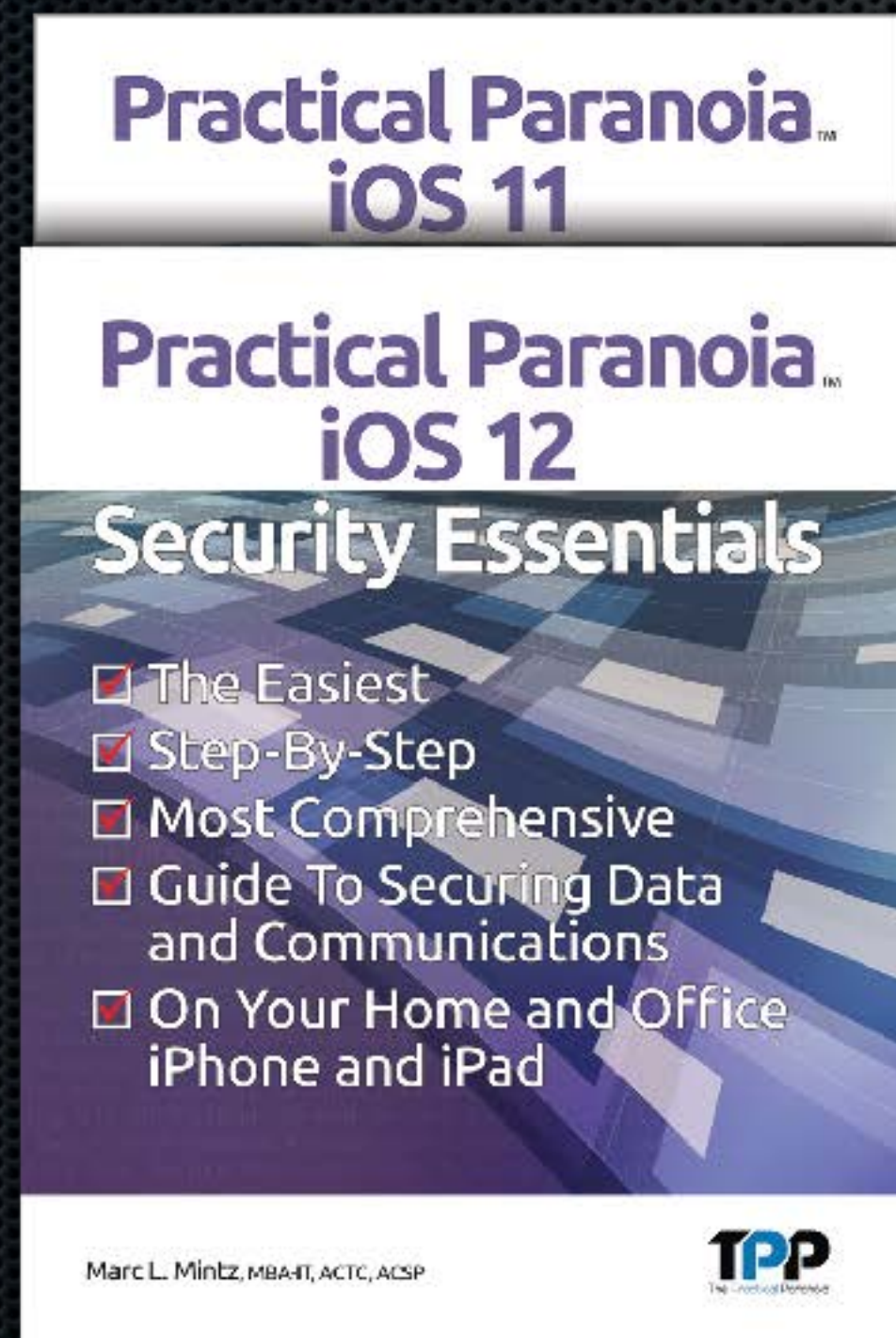


Practical Paranoia Security Essentials

Marc Mintz, MBA-IT, ACTC

505.814.1413 • marc@mintzit.com



Marc Mintz, MBA-IT, ACTC

- ✦ President, Mintz InfoTech, Inc.
 - ✦ Virtual CIO and IT Department for businesses throughout New Mexico
- ✦ Author, Practical Paranoia Security Essentials books for iOS, macOS, and Windows



The Threats

Just because you're paranoid doesn't mean they aren't after you

–Joseph Heller, *Catch-22*



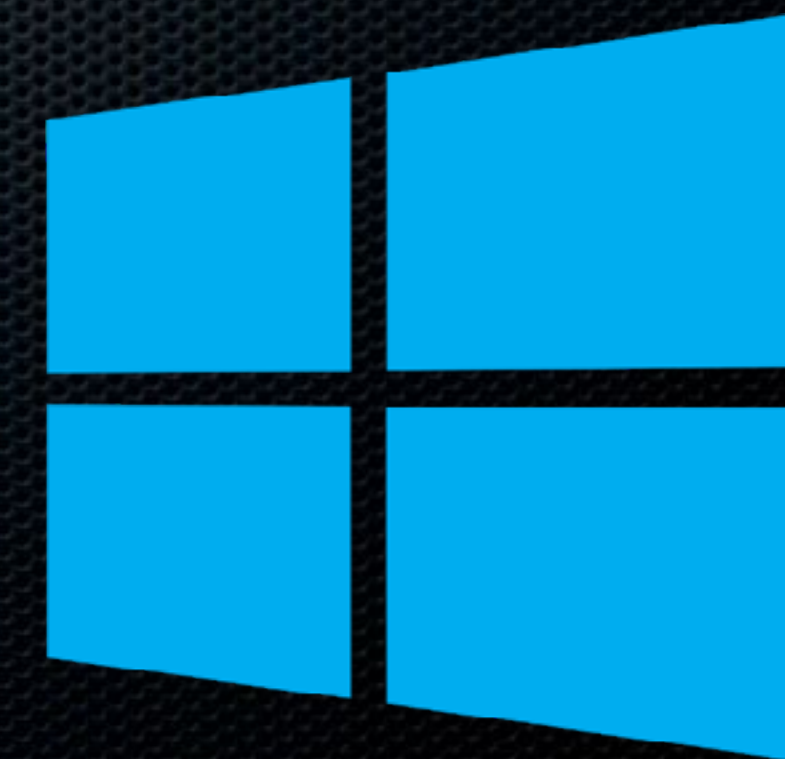
The Threat: Malware

- ✦ 4,000,000-40,000,000:
Number of known malware in
the wild
- ✦ Unknown number of
unknown malware
- ✦ Antivirus software catches
only 99.9% of *known*
malware



The Threat: Criminal Hacking

- ✦ Out of the box, all computers and mobile devices are vulnerable



The Threat: Interception

- ✦ The Cyber Intelligence Sharing and Protection Act (CISPA) promises the government unrestricted access to all of your cellular and digital data
- ✦ Business competitors, tech-savvy kids, and criminals can easily intercept phone calls, instant messages, email, network traffic, and your device
- ✦ Amazon, Facebook, Google business model is to harvest and then sell your information



Points of Vulnerability

*Knowledge, and the willingness to act upon it,
is our greatest defense.*

–Marc L. Mintz



Your Computer or Mobile Device

You



- Millions stolen every year
- Password easily bypassed
- Virus and malware infection
- Criminal penetration
- If sending email, your username, password, and text may be clearly visible
- Website visits are tracked to the pixel



From Your Device to WiFi or Cellular

You

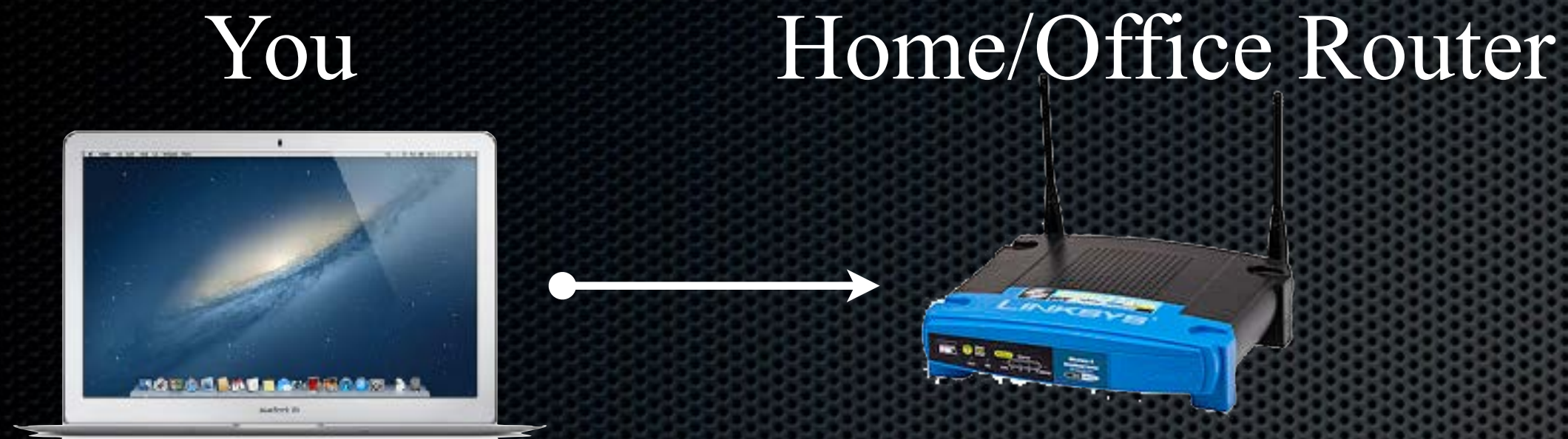
Home/Office Router



- Most WiFi networks have either:
 - No encryption
 - WEP encryption which is easily broken
 - Default password
 - Out of date firmware
- Millions of routers and modems are compromised



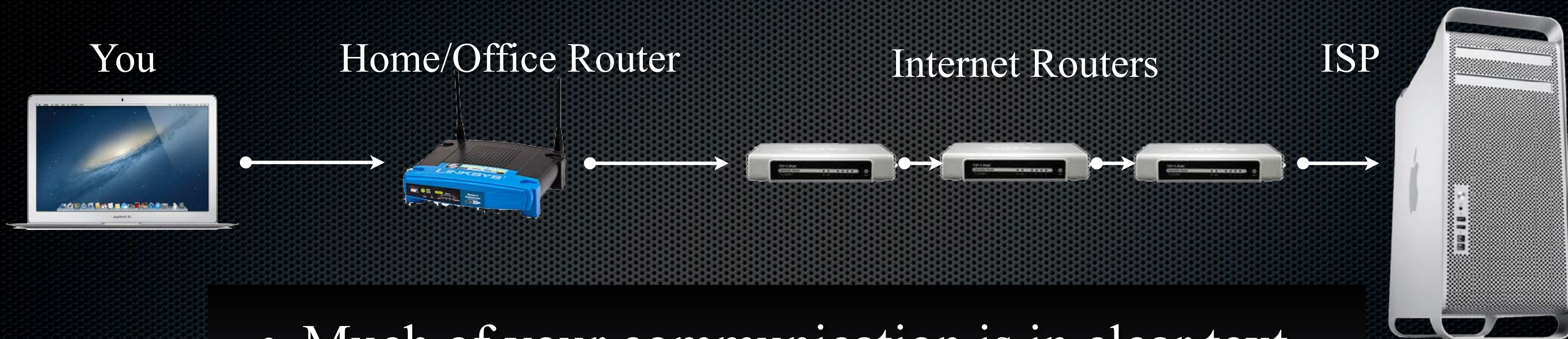
From Your Computer to Ethernet



- All data—including usernames and passwords—traveling along Ethernet can be easily intercepted
- Ethernet cable is a huge broadcast antenna
- Accessing the router using default credentials or cracked credentials



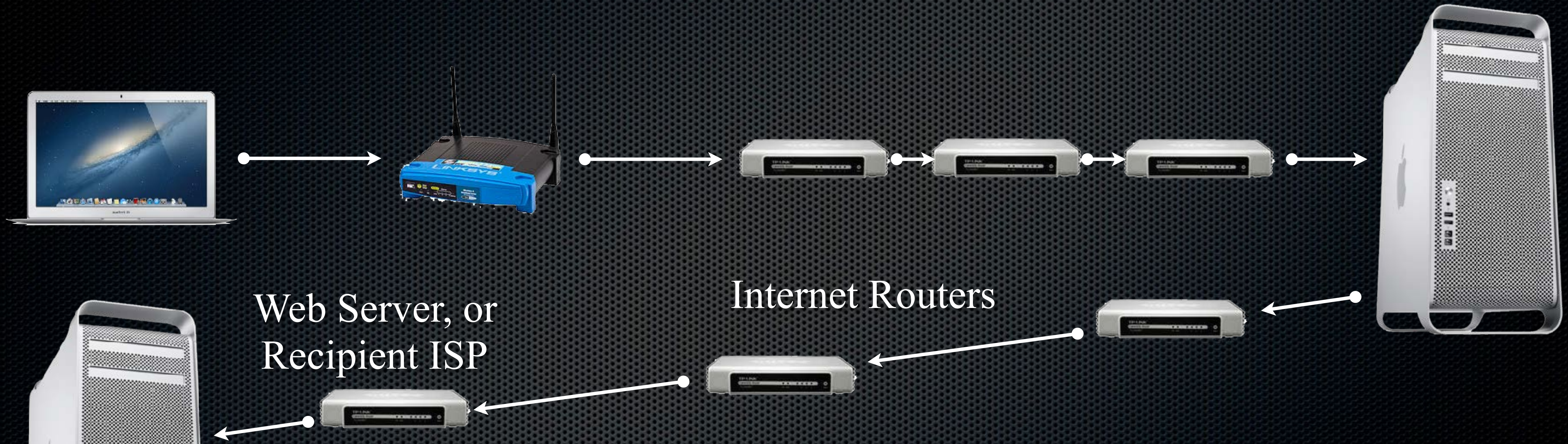
From Local Network to ISP



- Much of your communication is in clear text, readable by anyone at any of the dozens of routers along the way
- ISPs commonly monitor your traffic, and more specifically, your data

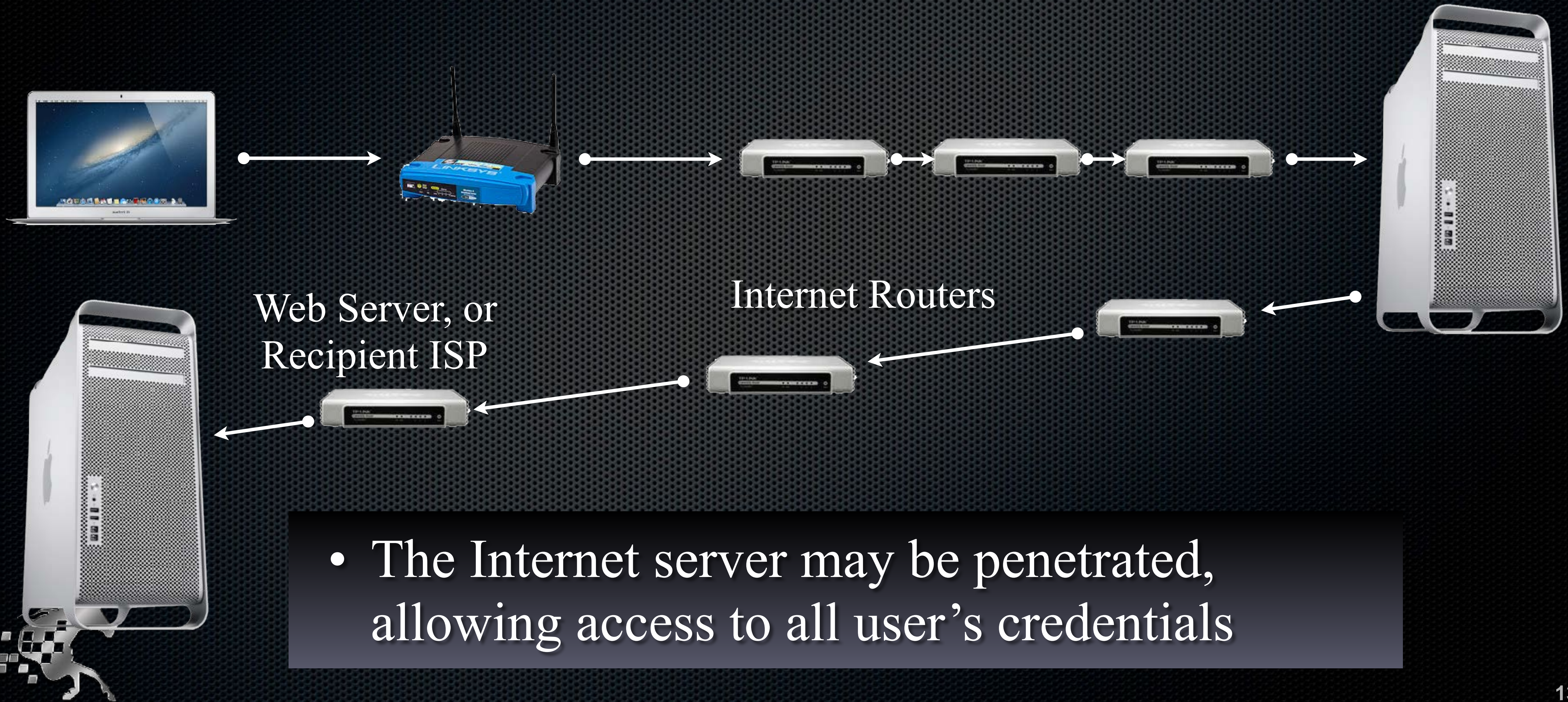


From Your ISP to the Internet



- From your ISP servers to the Internet, on to the target server, anyone at the dozens of routers along the way have access to your data

From Your ISP to the Internet



- The Internet server may be penetrated, allowing access to all user's credentials

From Sender to Recipient

- In the case of email, phone call, video call, and text message, the message may be clearly visible along the entire route, right up to your recipient
- There is no confidence that the intended recipient is the only one reading the email



The Sky Is Falling! Build a Plan Of Action

No matter how paranoid or conspiracy-minded you are, what the government is actually doing is worse than you imagine

– William Blum, former State Department employee



NIST 800-171

- ✦ No need to reinvent the wheel
 - ✦ Federal Government cybersecurity best-practices
 - ✦ 120 checkboxes to build your Plan Of Action & Milestones
 - ✦ *Does not* provide guidance on *how* to do it



Password

- ✦ Current cracking software and hardware can make over 10,000,000,000 password attempts per second from a single computer.
- ✦ Always use strong passwords
 - ✦ Definition: Minimum 15 characters
- ✦ Use a different password for each web site and service
- ✦ Check for account hacks at haveibeenpwned.com



Password

- ✦ *Don't* use biometrics for device login
 - ✦ Your device is covered with your fingerprints
 - ✦ Facial ID can be forced




Password

- ✦ Enable *Password Policies* for all computers and mobile devices:
 - ✦ Computer: Minimum 15 characters
 - ✦ Mobile Device: Minimum 15 characters, or minimum 6 characters with full erase after 10 failed attempts
 - ✦ Cannot reuse password



LastPass

- ✦ Autogenerate, remember, and autofill strong passwords
- ✦ Synchronize across all browsers
- ✦ Synchronize across Android, iOS, macOS, Windows



The image shows a screenshot of the LastPass website. At the top, there is a navigation bar with the LastPass logo and a "Get LastPass Free" button. Below the navigation bar, there is a banner with the text "NEW! LastPass Enterprise now offers seamless log in with Active Directory credentials. Learn more >". The main content area features the headline "Simplify your life." in red, followed by the sub-headline "LastPass remembers all your passwords, so you don't have to." Below this, there is another "Get LastPass Free" button and a link to "Upgrade to Premium for just \$2/Month >". At the bottom, there are three browser window mockups: Facebook (showing a password field), Amazon (showing a shipping address field), and Salesforce (showing a password generation field).

User Accounts

- *Everyone* logs in with a non-administrator account
 - Recommend all end-users have Parental Control (macOS) or Child (Windows) account



User Accounts

- Enable *Application Whitelisting* within Parental Control and Child accounts
 - Blocks malware not caught by antivirus



User Accounts: Administrators

- ✦ Only those authorized and with need to know have access to administrator credentials
 - ✦ Being a manager or leader is *not* need to know



Data Loss

- ✦ At least 1 on-site backup
 - ✦ macOS: Time Machine or CarbonCopyCloner
 - ✦ Windows: Acronis True Image
- ✦ At least 1 off-site backup
 - ✦ Code42
 - ✦ SpiderOak
 - ✦ Google Backup & Sync with Google Vault



System and Application Updates

- ✦ Why are there updates?
 - ✦ Bug fixes
 - ✦ Feature enhancements
 - ✦ ***Security holes plugged***
- ✦ Imperative to maintain updates to the OS and all applications



System and Application Sources

- ✦ There are more malicious than legitimate application download sites
- ✦ Purchase or download only from a vetted vendor



Storage Encryption: FileVault 2 (macOS)

- ✦ The most important upgrade feature of macOS 10.7-10.14
- ✦ Enables military-grade full-disk encryption for all writeable disks



Storage Encryption: BitLocker (Windows)

- ✦ Enables military-grade full-disk encryption for Windows storage devices
- ✦ Requires:
 - ✦ Windows 10 Pro
 - ✦ TPM chip (business-class PC)
 - ✦ Not sure? *Windows + R, type `tpm.msc`*



Sleep & Screen Saver

- The second you walk away from your computer, it is vulnerable to physical access
- Configure Sleep & Screen Saver to require password after 10 minutes
- Put computer to Sleep or Screen Saver when walking away



Anti-Malware

- ✦ Even the best anti-malware catches only 99.9%, letting through up to *40,000 known* malware, and countless *unknown* malware
- ✦ Installation of quality anti-malware is critical
 - ✦ We only recommend *bitdefender.com*
 - ✦ Bitdefender Gravity Zone for business
 - ✦ Bitdefender Central for non-business



Anti-Malware: Websites

- ✦ It is now easier to infect websites than end-user computers
- ✦ Criminals compromised websites, which then attempt to compromise your computer
- ✦ Use Bitlocker Trafficlight plug-in for all browsers



Firewall

- ✦ The Firewall prevents unauthorized network eyes from accessing your computer
 - ✦ Android: Requires rooting for firewall access
 - ✦ iOS: No firewall, no need
 - ✦ macOS: Out of the box, Firewall is turned off
 - ✦ Windows: Out of the box, Firewall is turned on
 - ✦ Router: Verify is enabled with Stateful Packet Inspection



Firmware Password (macOS) BIOS & UEFI Password (Windows)

- ✦ A hacker can break into your Computer in under a minute by booting from another source
- ✦ Prevent this by installing a Firmware/BIOS/UEFI Password
 - ✦ **Warning:** If this password is lost or corrupted on macOS, you *must* have original purchase receipt for reset



Lost or Stolen Device

- ✦ Android: Find My Device
- ✦ iOS: Find My iPhone/iPad
- ✦ macOS: Find My Mac
- ✦ Windows: Bitdefender AntiVirus
- ✦ Universal: Prey



Local Network

- ✦ Use a router with Intrusion Protection System (IPS)
- ✦ Enable WPA2 with AES
 - ✦ Never use WEP or TKIP
- ✦ Use strong passwords
- ✦ Change device default administrator credentials
- ✦ Power-cycle monthly
- ✦ Update firmware monthly
- ✦ Verify no unnecessary port forwarding or DMZ
- ✦ Use a separate Guest network for guests
- ✦ Only allow authorized devices that have passed security audit



Local Network

- ✦ Our current network darling is *Ubiquiti*
 - ✦ Enterprise-grade
 - ✦ Hardened security
 - ✦ Easy user interface
 - ✦ Monitor most activities
- ✦ Certified administrators
- ✦ Constant firmware upgrades
- ✦ Cloud-based management
- ✦ Routers, Access Points, Switches, and more



Web Browsing

- ✦ Install HTTPS Everywhere
- ✦ Use DuckDuckGo search
- ✦ Install Ghostery anti-tracker
- ✦ Install Bitdefender Traffilight
- ✦ Enable browser Do Not Track
- ✦ Enable browser Block 3rd-party cookies
- ✦ Change browser fingerprint
- ✦ Enable browser Fraudulent Website Warning
- ✦ Use strong, unique passwords
- ✦ Use 2-Factor Authentication
- ✦ Check monthly for account hacks at haveibeenpwned.com



Email

- ✦ All email accounts must use either TLS or HTTPS
 - ✦ Verify other party with checktls.com
 - ✦ Force TLS with paubox.com
- ✦ Never click a link without verifying URL
- ✦ SPF, DKIM, and DMARC records created
 - ✦ Requires personal domain name
- ✦ Enable 2-Factor Authentication



Voice, Video, and Text

- ✦ Use Wire.app or wire.com
 - ✦ Includes voice, video conference, and instant messaging
 - ✦ Works with Android, iOS, macOS, Windows, and browser
 - ✦ Military-grade encryption for all of your communications



Internet Activity

- ✦ Normal network and internet traffic can be viewed and harvested from miles away
 - ✦ Military does this from 600 mile high satellite
- ✦ Install and use VPN to block understanding of the traffic from device to the VPN server
 - ✦ NordVPN
 - ✦ Perfect Privacy



Social Media

- ✦ Create HR policies for proper use of Social Media
- ✦ Strong, unique password for each site
- ✦ Enable 2-Factor Authentication
- ✦ Review all privacy settings
- ✦ Remove unneeded site-associated apps and games
- ✦ Review all ad settings



When It Is Time To Say Goodbye

- ✦ Remove Firmware/BIOS/UEFI password
- ✦ Mac & iOS remove from iCloud approved device list
- ✦ Create a clone backup
 - ✦ Mac: CarbonCopyCloner
 - ✦ Windows: Acronis True Image
- ✦ Secure erase the storage device
 - ✦ Unencrypt device
 - ✦ Parted Magic for greater security



IT & CIO Support

Marc Mintz, MBA-IT, ACTC

505.814.1413 • marc@mintzit.com

mintzit.com • thepracticalparanoid.com

**Practical Paranoia™
iOS 11**

**Practical Paranoia™
iOS 12**

Security Essentials

- ☑ The Easiest
- ☑ Step-By-Step
- ☑ Most Comprehensive
- ☑ Guide To Securing Data and Communications
- ☑ On Your Home and Office iPhone and iPad

Marc L. Mintz, MBA-IT, ACTC, ACSP

TPP
The Practical Paranoid

**Practical Paranoia™
macOS 10.13**

**Practical Paranoia™
macOS 10.14**

Security Essentials

- ☑ The Easiest
- ☑ Step-By-Step
- ☑ Most Comprehensive
- ☑ Guide To Securing Data and Communications
- ☑ On Your Home and Office macOS

Marc L. Mintz, MBA-IT, ACTC, ACSP

TPP
The Practical Paranoid

**Practical Paranoia™
Windows 10**

Security Essentials

- ☑ The Easiest
- ☑ Step-By-Step
- ☑ Most Comprehensive
- ☑ Guide To Securing Data and Communications
- ☑ On Your Home and Office Windows Computer

Marc L. Mintz, MBA-IT, ACTC, ACSP

TPP
The Practical Paranoid



Recommended Vendors

Service/Product	Company	Contact	Email
IT Security	Mintz InfoTech, Inc	(888) 479-0690	marc@mintzit.com
DIY IT Security Books	The Practical Paranoid	(888) 504-5591	info@thepracticalparanoid.com
Anti-Virus	Bitdefender		https://bitdefender.com
Routers	Ubiquiti		https://ubnt.com
IT Best Practices/ POAM	NIST SP800-171		https://csrc.nist.gov/publications/detail/sp/800-171/
Password Manager	LastPass		https://lastpass.com
Secure Voice, Text, Video	Wire		https://wire.com



Recommended Vendors

Service/Product	Company	Contact	Email
On-Site Backup	macOS: bombich.com Windows: acronis.com		https://bombich.com https://acronis.com
Cloud Backup	Code42 Spideroak Google Backup & Sync		https://code42.com https://spideroak.com https://www.google.com/drive/download/backup-and-sync/
Full Disk Encryption	macOS: FileVault2 (built-in) Windows: BitLocker (built-in Windows 10 Pro)		



Recommended Browser Extensions

Service/Product	Company	Name
Malicious Website Block	Bitdefender	Trafficlight
Force HTTPS Secure Connection	Electronic Frontier Foundation https://www.eff.org/https-everywhere	HTTS Everywhere
Secure Search	DuckDuckGo.com	DuckDuckGo
Block Trackers & Fingerprint	ghostery.com	Ghostery



Recommended Email Security

Service/Product	Company	Name
Hacked Internet Accounts	haveibeenpwned	https://haveibeenpwned.com
Verify Email TLS Encryption	check-tls	https://check-tls.com
HIPAA & SEC Compliant Encrypted Email	Paubox	https://paubox.com



Recommended VPN

Service/Product	Company	Name
VPN	NordVPN	https://nordvpn.com
VPN	Perfect-Privacy	https://perfect-privacy.com

