Securing Client Data

Best Practices for Curating Third-Party Information

WOODARD™

During this Training Event You Will…

1. Explore ways to securely exchange and store login information between you and your clients – including updates to passwords and multi-factor authentication codes
2. Learn key elements of a privacy and data management policy and strategies to manage adherence to these policies within your practice
3. Discover ways to maximize security with your practice's cloud document management systems, local computers, and mobile devices

Segment 1

Explore ways to securely exchange and store login information between you and your clients

Security is a human Issue, not an IT one

Same Password For Accounts

67% of all Americans use the same password for different online accounts

Source: Security.org

Personal Password Blending

54% of workers use the same password for their job and personal apps

Source: Yubico

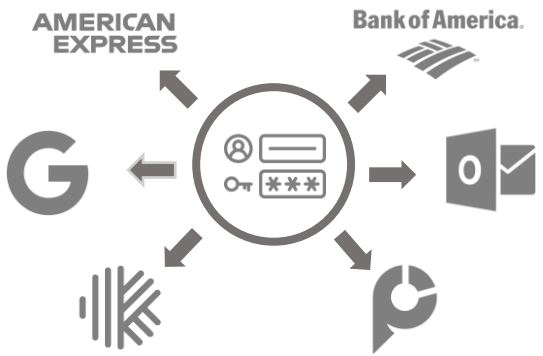
Data Breaches Due To Poor Password Security

80% of data breaches are due to poor password security (reused & weak passwords)

Source: Verizon Data Breach Report

Risks

Browser / Retail Password Managers



Daisy Chaining Passwords

Sharing Across Devices (Blending)

Controls

Granular Control by Team Member
(as- needed access)

Tracking Usage by Team Member

Single-Click Lock Out

Shared Documents
(even if password-protected)

3 Pillars of Password Security

Tech – Implement tools to make it easy and secure

Team – Train your team so that they understand their responsibility

Policy – Back up the training with written policies

Segment 2

Key elements of a privacy and data management policy

Key Elements of a Privacy and Data Management Policy

A Conversation with Joe Woodard and Jamie Beresford

Note: This segment is audio only.

Segment 3

Maximizing security with your practice’s cloud document management systems, local computers, and mobile devices

Best Practices for Maximizing Security

Practice 1: Email Policies and Procedures

- Never open any unexcepted file attachments to an email
- Never click any link in any email…ever
- Tip: Use secure and collaborative systems for communications and files (e.g., Slack, Liscio, or MS Teams)
- Tip: Include personal references in emails with attachments and links to validate the sender…but be careful
- Tip: Use phishing protection solutions (e.g., Iron Scales)

Note: Fax is even less secure than email, and VOIP conversations that are not protected by firewalls can be as vulnerable as email!

Best Practices for Maximizing Security

Practice 2: Data Hosting and Storage

- Data stored in the cloud is the safest container…assuming it is a state-of-the-art container of course!
- However, almost all providers allow for locally mapped/synchronized folders
- Microsoft is the best option for local synchronization because:
  - Remote Device Management (e.g., Active Directory) provides centralized control of the device
  - There are options to map files but not push them to local devices

Best Practices for Maximizing Security

Practice 3: Information Technology Management

- Microsoft Azure Active Directory → Device Management
- Microsoft Intune → Device Management
- Collaborative File Structures (e.g., Microsoft SharePoint or Google Drive)
- Tip: Eliminate all local file servers
- Tip: Use company management devices for laptops and tablets and at least MDM on personal cell phones

Best Practices for Maximizing Security

Practice 4: Hardware Management

- Update Devices Regularly
  - Developer Updates (e.g., firmware and BIOS)
  - Operating System Updates (PC and Mobile)
- Don’t Use Digital Printers and Digital Copiers in Public Locations (e.g., FedEx, UPS Store, etc.)
- Tip: Destroy Hard Drives after Deprovisioning Hardware Devices

Best Practices for Maximizing Security

Practice 5: Home and Office Networks

- Use a company managed software firewall (e.g., AVG, Sophos Home, Webroot, etc.)
- Consider hardware firewalls (e.g., Unified Dream Machine)
- Use Ethernet for company managed devices
- Use Virtual Private Networks (VPN) solutions like Open VPN

Tip: Don’t locate your wireless router near your work location due to electromagnetic radiation.

Best Practices for Maximizing Security

Practice 6: Data Encryption

- Deploy Bit locker for Microsoft computers. Apple has similar options for data encryption on local devices
- Protect the transfer of information through SSL at a minimum of 256-bit encryption levels

Best Practices for Maximizing Security

Practice 7: Identity Management

- Deploy Multi-factor Authentication, preferably with bio-readers like face and/or fingerprint
- Use an authentication application like Microsoft Authenticator or Google Authenticator – layered with bio-reader identity verification
- Note: Solutions like Microsoft Active Directory assist with local user identity validation as well

The Big Question!

What if you could fully protect yourself and your clients using all the strategies in this webinar in just 10 weeks?

About the Microsoft Implementation Boot Camp

- Deploy, or expand your use of, Microsoft 365 in your business, including transferring email and files if applicable.
- Protect team collaboration, client collaboration, document sharing, and practice/client information.
- Centralize information through comprehensive Microsoft Cloud utilization.
- Adopt best practices for the use of Microsoft 365 throughout your organization.

www.Woodard.com

WOODARD™

Practice Protect Data Security Plan

https://practiceprotect.com/data-security-plan/

Securing Client Data

Best Practices for Curating Third-Party Information

WOODARD™