DEFEND AGAINST HACKING, PHISHING, AND SPOOFING ATTACKS

Financial Advisors are Attractive Targets

Online "hacktivists" are gaining worldwide notoriety for their hacking exploits. While attacks on banks and financial institutions make headlines, unpublished attacks are directed at financial advisors every day, with some resulting in significant financial losses and also the loss of client trust. Take the necessary steps to decrease your vulnerability to external threats. Learn about tools and techniques that can help you minimize your firm's and your clients' chances of becoming a victim of a well-engineered attack.

Login Security

Secure all of the devices and online services you use with strong passwords. Hackers will attempt to crack your passwords with brute force attacks using combinations of dictionary words, common number and letter substitution (@ for "a"), and pattern checking.

- The illustration at http://xkcd.com/936/ demonstrates how many of us have been incorrectly led to believe that mixing case and performing character substitution increases password strength.
- The key to password strength is **entropy**, or measure of uncertainly in random variables.
- The more characters in a password, the higher its entropy. Clearly, length equals strength.
- Passwords are like boxer shorts: Change them often, don't share them, don't leave them lying around, and keep them a mystery!
- Use http://www.passwordmeter.com/ for password (or a close approximation) strength ratings.
- Many of us have dozens of passwords for all the various websites and services we use. Popular password manager software helps organize and secure passwords, including:
  - LastPass
  - RoboForm
  - Dashlane
  - 1Password
  - Meldium

In addition to strong passwords, use multi-factor authentication for greater security to your online logins. There are three types of authentication factors to verify your identity:

- **Something You Know**, like your username, password, PIN, or finger gesture pattern.
- **Something You Have**, like your ATM card, security token, smartcard, or mobile phone.
- **Something You Are**, like your fingerprint, retina, voice, or typing rhythm.

Websites and services that support multi-factor authentication, typically using your mobile phone, include **Google**, **Facebook**, **LastPass**, **Dropbox**, **Twitter**, **LinkedIn**, **Chase Bank** and more.

When you use the Internet, be aware of your protection using security and encryption protocols.

- Whenever possible, connect to websites using an **https://** connection and Secure Sockets Layer (**SSL**) and Transport Layer Security (**TLS**). Modern browsers will display secure certificate information in the address bar.
- Enforce https:// connections with the **HTTPS Everywhere** browser plugin compatible with Firefox and Google Chrome.
- Attackers use programs like **Firesheep** and **WiFi Pineapple** to eavesdrop on unsecured http:// (no "s") connections to capture your online credentials and gain access to your accounts.

Device Security

Just as you secure your computers and online accounts with strong passwords, your mobile devices also need to have strong protection.

"If unlocking your device isn't a little inconvenient, it isn't secure."

- Enable the **passcode** login, activate the **Auto-Lock** timeout, and set the number of failed login attempts before device information is erased.
- Turn off the default four-digit passcode (iOS) or login pattern (Android) and replace it with a longer alphanumeric one. If unlocking your device isn't a little inconvenient, it isn't secure.
- Be familiar with apps to locate and remotely wipe a lost or stolen device. For iOS, use **Find My iPhone**, Blackberry use **BlackBerry Protect**, Windows use **Exchange ActiveSync**, and Android use **Android Device Manger**. Third-party apps include **Norton Mobile Security**, **Lookout Security**, **avast! Mobile Security**, or an app supplied by your cellular carrier.
- Enterprise mobile device management platforms include **Symantec Mobile Management**, **AirWatch by VMWare**, **MobileIron**, **XenMobile by Citrix**, and **IBM MobileFirst** are built to support the Bring-Your-Own-Device (BYOD) trend in the workplace.

Safe Data Sharing

Would you mail a postcard containing a client's social security number or birthdate? No way! But what about sending the same information via email? **Email is not a secure way** to communicate personal information. You can attach files to emails that are protected with a password, but remember the **entropy** guidance earlier in this document.

Secure file exchange services are becoming popular methods to exchange confidential files. Services include **ShareFile**, **Box**, **SecureDrawer**, **SpiderOak** and **Wuala**.

Also confirm that the networks you use for business are secure.

- Contact a professional to review your **hardware and software firewall** settings. Perform "leak testing" of existing devices and document test results for your internal files.
- Secure your WiFi networks with **WPA2 encryption**. Require a **strong access password** (high entropy) for WiFi access, and **turn off your WiFi network** when it is not needed, such as overnight.

Social Engineering

Attackers use social engineering techniques to manipulate people into divulging confidential information. Popular social engineering techniques include:

- **Phishing:** Typically an email that is carefully crafted to appear like it came from a trusted source, but contains links to websites designed to capture your personal and confidential information.
- **Pretexting and Spoofing:** Attackers impersonate a close friend, relative, or client in a ruse to get you to offer personal information you would only provide to someone you know.
- **Reverse Social Engineering:** Attackers contact you claiming to represent a software company and that your computer has a problem they detected. They offer to fix the problem with a software update, but the software update is malicious software (malware) designed to steal your information.
- **Curiosity:** Attackers drop USB thumb drives with enticing labels (e.g. "Personal and Confidential," "2014 Tax Returns") in business parking lots, hoping people will pick them up and plug them in to corporate computers to read their contents. This allows attackers to deploy malware inside the corporate firewall.

Attackers create a false sense of urgency to pressure or scare you into doing something they want. They use fear tactics or temptation to compel you to act when you shouldn't. Common sense strategies are often enough to defend against social engineering tactics.

"Attackers want you to act without thinking. If a situation doesn't 'feel' right, pause and gather your thoughts."

- **Be Suspicious:** Consider the context of communication. Is the message sudden and unexpected?
- **Stay Updated:** Keeping the software you use updated reduces the chances attackers can exploit known vulnerabilities to steal your information.
- **Resist Urgency:** Attackers want you to act without thinking. If a situation doesn't "feel" right, pause and gather your thoughts. Anxious attackers will give up quickly.
- **Authenticate and Verify:** Ask to call back the alleged attacker impersonating a client. Challenge the caller with a security question, or send a verification code to their mobile phone.
- **Training:** Conduct simulated phishing attacks in your business to identify vulnerable points of contact. Solutions include **Wombat Security**, **TraceSecurity**, and **ThreatSim**.

If you believe you are a victim of an attack, contact your custodian and/or broker-dealer, your client(s), and the **Internet Crime Complaint Center** (IC3). The **FTC Identity Theft Resource Center** also has useful material.