Apr. 22, 2016

Personal documents and data are an identify thief's dream...their ticket to accessing financial accounts, applying for loans and credit cards, and other credit-destroying behavior. Take this a step further to include tax documentation, and now you've got a one-stop shop for social security numbers, employer and financial information, addresses, and employer identification numbers.

It's personally identifiable information to the extreme. The fact is that scammers are

Common data-compromising positions

There are so many ways scammers can get to data. Being aware of these tricks is the first step in protecting your firm and your clients.

Social engineering: This is an all-too-common method that tricks individuals into giving out personal information. In fact, this method is so effective that it boasts an 80% success rate. Common scams include a phone call from "customer service" or an onsite visit from someone claiming to represent a company or agency and requesting personal information to solve a fictional issue. And no agency is safe from impersonation; just consider the sophisticated phone scam of 2014, where crooks posed as IRS agents demanding tax payments.

Phishing: This is simply the digital equivalent of social engineering where scammers impersonate a company or well-known agency online. Victims often receive an official looking email asking for their personal information or are invited to click a link that leads to a phony website designed to capture personal data.

Physical access/shoulder surfing: This is exactly what it sounds like. If scammers can access your hard copy documents or your computer, then they can easily get to your personal information. Don't be surprised either if your information is stolen by someone simply looking over your shoulder and surfing your device's screen. Scammers have even been known to use mirrors to read computer screens with their backs turned to the victims. All too often, individuals get lost in their technology and forget that their data is exposed.

Expired access: Many businesses forget to remove former employees or contractors from their systems after these folks depart, opening the door to data theft. The fact is

that most system hacks are inside jobs, performed by former and/or disgruntled

or expired antivirus software and networks that are unsecure and wide open, such as public WiFi. Security weaknesses are bait for scammers at the ready to track key strokes, capture unencrypted data, and flog users with ransomware.

Data-protecting tips

For all the scams identified above, there are basic tips that help bar attackers from infiltrating your firm. This information is also gold in supporting ongoing education for clients.

Outsmart the social engineers and phishers: The basic rule is to never give sensitive information to anyone just because they ask. Legitimate inquires most often will come via mail, and rarely by phone or through email. Challenge inquiries by asking requestors to verify their identity and then direct them to send the request via mail.

Secure your physical fortress: You heighten the security of both hard and electronic documents and data by simply limiting access. Enforce strict onsite visitor policies (require badges and sign-in), lock file cabinets and encrypt documents, secure computers with complex passwords (and change your passwords regularly), and install privacy screens on all devices.

Eliminate expired "goods": We throw out expired milk for fear of the nauseating physical consequences, so why do we put our personal data at risk by maintaining logins for expired staff? The consequences are just as nauseating. Avoid the data-theft plague by establishing a structured security policy. Strictly enforce rules for who has access to what information, and adhere to the "principle of least privilege"—give the minimum access required to perform the job. Also, be sure to discontinue system access immediately after an employee, contractor, or vendor no longer requires it.

Clean out your dumpster: Keep scammers out of your physical and digital dumpsters by destroying information up front. Shred paper docs and wipe all media including

disks, drives, and other devices.

While many of these data-protection tips seem common sense, it's surprising how many people do not employ them. The consequences of being hacked can be devastating to both your firm and your clients, so take heed and proceed with caution by applying these tips, while also reviewing the IRS guide, "Safeguarding Taxpayer Data" (https://www.irs.gov/pub/irs-pdf/p4557.pdf). Avoid the "Big Take" by shutting down attackers before they infiltrate.

Firm Management • Taxes • Technology