# Protect Your Law Firm From a Social Engineering Fraudster

If you thought the picture above was of Barack Obama, look again. It is not President Obama. It is an impersonator. Impersonation is one of many ways that social hackers are using technology to defraud attorneys across the globe. Hackers used to be highly technically skilled people who were proficient at using their technology skills to get into accounts that did not belong to them. Once hackers were in accounts, all manner of stealing took place from unauthorized money transfers to fraudulent credit accounts established with the help of identity theft. This new form of social hacking, socially engineered fraud, uses the power of the internet to leverage relationships to overwhelm victims.[1. ©2016 Brandon L. Blankenship, Image Credit: Barack Obama impersonator by Gage Skidmore CC flickr 18 June 2011.]

Today, hopefully, there aren't any attorneys left that might fall victim to emails from strangers (especially Nigerian strangers) requesting help with a financial matter. What attorneys are falling victim to, however, are socially engineered attacks. Now the email comes from a friend or a family member who knows a lot about you. It might start something like this, "It was good to see you at the reunion last week. A bunch of us are talking about sending money to our friend Greg to help him through his recovery …"

The catch is - the email is not from a friend or a family member. It is from a Social Engineering Fraudster.

The latest hidden enemy, the Social Engineering Fraudster, has better emotional skills than technical skills. Every day they refine the art of influencing people to disclose information that they shouldn't and do things that they ought not do but are willing to do for a friend or someone they trust.

The Social Engineering Fraudster usually starts by trolling social media (LinkedIn, Facebook, Twitter, Etc.) for a potential victim. Once a victim is identified they use social media to learn as much as they can about the victim and the victim's social and business networks.

## Over Half of Businesses Globally Have Been Victimized

Nearly half of global businesses surveyed reported being the victims of one or more social engineering attacks.[2. Guide to Preventing Social Engineering Fraud, Chubb.] There are many examples of a socially engineered attack. One example may be impersonation. By using resources that are accessed for free on the internet, a Social Engineering Fraudster can learn enough to impersonate a victim. While impersonating a person of authority, employees can be instructed to wire funds or transfer assets, release confidential information or proprietary information.

Another example is **vishing**. Imagine that you finance a car through Big Bank. The next day, you receive an automated call from Big Bank. The caller I.D. shows "Big Bank." The automated voice

announced that the call is from Big Bank. It goes on to thank you for trusting Big Bank with your financing needs and asks you to confirm the first three numbers of your social security number. If you punch them in, you just became the victim of vishing. The Social Engineering Fraudster already had the last six number of your social security number. The first three digits of your social security number had been blacked out on a traffic ticket you got ten years ago. Now that the Social Engineering Fraudster has your complete social security number they can start getting credit cards issued in your name. A few simple steps can establish a human “firewall” against socially engineered attacks. Here are four of them.

## Use Emails You Know

When you get an email from someone purporting to know you, resist the convenience of simply clicking reply. Instead, start a new email and use the email from your contacts, the email that you regularly use. Social Engineering Fraudsters often use a fake email to communicate. It is masked to look right, but it isn’t.

## Verify Transactions By Phone

Before you make a wire transfer or payment for a client, verify the payment information with your client by phone (or in person). Again, use the phone number from your contacts rather than one that is provided to you.

## Verify Information Changes

When a person requests that you change information in your payment or access systems, verify the information change request from someone other than the requestor.

## Create an Aware Culture

Social Engineering Fraudsters use their high level of emotional skills to select victims. Everyone that comes in contact with your law firm is a potential victim. If the managing partner is not accessible, an IT gal that has access to the managing partner’s email will do. Consider buying lunch for everyone in your firm once a month. During lunch have a presentation that educates everyone about the latest socially engineered fraud schemes. If everyone is watching for an attack, it is hard for a fraudster to penetrate your firm. If you use contracted services, remember to include them in the process. Some vendors have as much access to internal systems as employees.

It is only a matter of time before a Social Engineering Fraudster makes an attempt on someone in your firm, your firm, or one of your firm’s clients.
### Brandon L. Blankenship