All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Fishing and phishing

I have been phishing almost as long as I have been fishing. I started fishing when I was in camp at perhaps 8 or 9 years old. We gathered our gear and went down to the stream, which was technically a tributary to a river, and cast away. I was a teenager when I first used email. When I was taught how email worked, it was obvious to forge email to get desired behaviors from recipients. We didn't call it phishing then, of course. We called it email forgery.

A skills sport

Fishing is a skills sport, and I never was good at it. It requires some combination of patience, which I don't have much of, and a sense of when to go easy and when to yank, which I also don't have. I tend to reel in when I should wait and wait when I should reel in. It is a skill acquired over time and perhaps taught, but I never learned it.

Phishing on the other hand is much easier, at least for me, because the Internet is full of folks who will bite on almost anything. Evolution has not killed off the easy targets yet. If it looks like an Apple email and sounds like an Apple email, it must be an Apple email. Completely false, but nevertheless how phishing succeeds. Maybe I just have skills in mental sports (games?).

Different types of fishing and phishing

Fly fishing was my favorite because I enjoyed the casting. You can aim where you want, develop the skill to deliver the baited hook to the desired point of entry, and with practice, you improve. I liked the physicality of it, and that, to me, was the fun of it. I liked fly casting and still do. On the other hand, tossing a line out there without the whipping back and forth never really appealed to me, even though on a windy day it certainly seems to do better.

Spear phishing is increasingly popular today, perhaps because it works better on a per cast basis, even though casting a wide net seems to work well enough to make it profitable. The real advantage of spear phishing is that you use intelligence processes to identify things likely to work in the particular situation and focus on the desired targets.

Catching

I never actually caught a fish. I remember one day at my uncle Bill's farm when we fished for about an hour with one of his cousins. I didn't get a nibble while he fished the pond out. Same bait, rod, reel, … everything but the fisherman. The last time I fished was a few months ago off shore near Bird Rock, and true to form I didn't catch anything. But I don't go for the fish.

Spear phishing increases the odds of success substantially, but the time and effort to do it well makes it only useful today for those with more to gain than a bit of money. When you can make millions in a year in the old Nigerian spam scam, why bother spearing a big fish.

Summary

Fishing and phishing are largely about the skills of the person and the fish. If we want to stop getting caught all the time, we should evolve (train) the fish. But that won't stop the sport or the dedicated phisher from spearing a big fish once in a while. Nothing will. However...

Basic training

Phishing is basically simple. It goes like this:

[Headers]

[Dear Someone]

[Something you want to hear]

[Something you should do]

[Click here to get it done]

[Close it out to look legitimate]

Your response options:

Best response: Click the “junk” icon in your email client

Worst response: Click on a link in the email message or reply to it

Some subtleties

Phishers are not all ridiculously obvious and foolish. They try to make their emails look like legitimate ones – in various ways. For example:

- **General appearance:** They try to make their emails look like “legitimate” emails from real sources. This ranges from a background color and a nice font to an exact match to a specific company's image, iconography, look, feel, etc.
- **[Headers]:** They try to make ”From:” and “To:” fields match expectations. This ranges from “From:” generic names (Julia, Bob, Ahmed, etc.) to known or celebrity names (Barack Obama), to names of people in authority (John Smith – VP of HR) to people you actually know (folks whose accounts they broke into along the way). The to field is (hopefully) you, but often enough it is a name that looks like the name of a mailing list (e.g., “Fisherman's Friend”) or the same as the sender. Subjects are often effectively deceptive (i.e., INVOICE / Late payment / Your lost credit card / etc.)
- **[Dear Someone]:** They try to make this either personalized (i.e., to you or someone else) or generic to a class of people (e.g., Dearest in God or Branch Managers and Tellers).
- **[Something you want to hear]:** I am a lonely young single woman looking for a friend in my time of need / I am a wounded warrior trying to return home / John said I could trust you to be an honest person / As part of a payroll system upgrade / etc.
- **[Something you should do]:** As you can see from my prom night picture ... / Help me get back to my family by … / Can you accept a wire transfer on my behalf? / Please update your employee details … / etc.
- **[Click here to get it done]:** If you send me your picture using Facebook / Send me money clicking on this miropayment site / Fill out this form with your details / Login and update your details … Typically each URL will be illegitimate but look like the real thing.
- **[Close it out to look legitimate]:** Thank you / Sincerely in Christ / Beloved friend / Sorry for the inconvenience …

How to tell the difference

There are almost always give-away hints. Here are some of them:

- **General appearance:** Most of them miss completely – hit the Junk button right away. If they are close, look for obvious misspellings of things like the company name.
- **[Headers]:** Headers you see should trigger suspicion if (1) you don't know them (2) they look different from the usual ones from that person, or (3) they are empty or contain garbage characters. Suspicion doesn't mean they are evil, but it means you should look more deeply at the rest of it. When in doubt, throw it out!
- **[Dear Someone]:** If it's not you or an actual group you are a member of, hit Junk.
- **[Something you want to hear]:** You are not the most attractive, trustworthy, helpful person in the world, and even if you were, they wouldn't know it. We almost all want to help others, but do it through a charity you know of and don't do it through email. Junk!
- **[Something you should do]:** Don't act now! Think about it first. If you still want to do it, do it by contacting a known organization through other means.
- **[Click here to get it done]:** Don't click! In most cases, an email from Microsoft won't point you to a site other than Microsoft.com. If you move your mouse over a link, it will typically show you the URL it points to. If it doesn't match the source of the email, don't go there. Also, rather than “click through”, you might try using the browser directly. For example, if it seems to be from your bank, use your browser to login to your bank without clicking on the email link. That way, no matter what they include in the link, it won't take you somewhere you don't want to go. Another approach is to look up the phone number using an independent means and call them. Don't trust the phone number in the email! If they are lying they might also give you a fake phone number.
- **[Close it out to look legitimate]:** Most fake close-outs are out of character for the actual people you know or organizations involved.

Some other hints

Don't ignore the obvious foolishness. For example these are things you are very unlikely to get in a legitimate email but are likely to see in a phishing email:

- The FBI needs your help, so they are emailing you
- Any taxing entity (the IRS, Canadian tax collector, etc.) is emailing you
- Someone you don't know owes you money and they want to use email to send it to you
- The person of your dreams who you have never met is trying to get in touch

Hopefully you get the idea.

Have no fear, trust but verify

You need not be afraid of email or spam or spear phishing.

Just like anything else, you need to be reasonable and prudent. Every once in a while you will get ripped off. But for the most part, a little bit of caution will keep you safe. You just need to learn to not always take the bait.

