

# The 5 Secrets to Phishing Success

Column by Mike Murray

These days, it's hard to perform a penetration test without attempting some sort of online social engineering, and most often, this takes the format of some type of phishing attack (whether targeted or across a wide user base).

While we spend epic amounts of time getting our exploits and payloads perfect (even if we're using SET), far too often we see testers using stock emails or variants of canned emails that they've been taught to use without thinking about the real keys to getting their emails read and acted upon.

These are my five most-often overlooked secrets to making sure that your email phishing works...

del.icio.us

Discuss in Forums {mos\_smf\_discuss:Murray}

## 1. THE SUBJECT LINE

The subject line of an email is much like your first impression - you will get away with nearly anything if you have a good one, and you'll rarely ever recover if you have a bad one. Unfortunately, most of us write bad email subject lines - our subject lines in SE situations tend to be vague and unimaginative.

While it's a natural instinct to want to be as unobtrusive as possible (i.e. when performing most SE engagements, we don't exactly strive to be memorable), this is exactly the logic that will get your emails moved immediately to the "trash" folder (especially if you do a bad job with the next four secrets).

Of course, the subject of the email has to be relevant to what you're attempting. If it's not, then you're going to be remembered (and you're going to get reported to the local security team by any moderately responsive workforce).

Phishing Scenario

Typical Subject Line

Good Subject Line

Fake Administrative Update  
Security Update  
Important: Patch Your Computer

Malicious PDF Document from a colleague  
The Documents you Requested  
Can you believe that he sent me this?

Direct to an entertaining malicious web link  
You should see this site  
Have you seen this one?

Protip: It's always good to instill some urgency in your target, but exclamation marks and heavy capitalization in your subject line scream "I'm a phishing email." Avoid them at all costs.

## 2. THE EMAIL ADDRESS

The number of phishing attacks that fail because the email address is too "phishy" probably is nearly innumerable. Many of us intuitively understand this and choose phishing emails that appear to come from the target domain; however, this can limit our ability to perform some of the scenarios that we may hope to accomplish.

This can all be avoided with heavy use of your GoDaddy (or other domain registrar) account and some creativity. Some ideas we have tossed around to make incredibly effective phishing email addresses have included the obvious ones (e.g. .net / .org analogues of our clients' domains) as well as some more esoteric tricks to replicate domains (internationalized domain names that have foreign characters that appear similar to the domain we're attempting to replicate).

An interesting one that we've actually used (effectively) was against a customer who we knew to be heavily dependent on Oracle products within their environment. In attacking their IT staff, we knew that a link sent from Oracle was likely to be acted on quickly. Of course, appearing as though we were Oracle was going to be somewhat difficult.

We also realized that the letters "c" and "l" placed next to each other look very much like a "d." So, we registered the domain "orade-support.com" (because "orade.com" was taken).

If you're creative, you can come up with any number of opportunities like this given who you're trying to impersonate.

### 3. SALUTATIONS

The salutation of an email tells us much about the sender and their intent. This all goes back to the way that we learned about letter writing when we were growing up &ndash; the difference between "Dear Mike," "Hi Mike" "Mike" and "To whom it may concern" is pronounced in our understanding of what is to follow.

This is one of the fundamental failures of most traditional phishing emails sent from overseas (especially those countries with school systems based on British English like India and Nigeria) &ndash; they tend to be far more deferential and formal in their salutations than those in the US and Canada are.

Imagine, for example, you are sitting at work and get an email from a co-worker that begins with, "Dear Esteemed Colleague." How suspicious would you be?

Similarly, choosing the correct salutation for your email (and, often, the answer "no salutation" is the right one) is required to ensure that your emails don't set off the target's suspicion.

### 4. SIGNATURES

Much like the salutation, we learned from a young age that we needed to sign our letters. Consequently, our reaction to the signature of an email is impressed deeply on our unconscious minds. The right signature can soothe a budding suspicion, while the wrong one will set off alarm bells in even the most otherwise perfect email.

As an example, take one of the companies that you interact with often (e.g. Paypal, Google, eBay, etc.) and examine the signatures that accompany each. You will likely discover a constancy of signature across the emails that unconsciously reassures you of who you're dealing with.

Likewise, you probably will notice that your friends all sign their emails in a similar way each time. For example, anyone receiving an email from me will notice that my notes are signed "-Mike" or "-M" nearly every single time. When I don't sign my notes that way, people notice.

And anybody attempting to impersonate me had better get that right.

## 5. TESTING YOUR EMAILS

There are two types of tests that every phishing email should be put through, before it hits the wire to ensure that it has the best chance of success. The first test is to ensure that your email will reach its target, while the second is about ensuring that you're being as appropriate as possible in the way that you write your email.

### Spam Assassin

Phishing attacks often fail for the stupidest reasons &ndash; chief among them is that the email is caught by the spam filters at your target domain. While this is what email filters are designed to do, it's easy to check your emails against industry standard spam filters like spam assassin before you send it.

When I'm crafting a phishing email, I'll often use my account at Aweber to test my email against their spam filters. They have an easy testing facility to perform that test.

However, if I didn't have an Aweber account, I'd use something like MailCheck to test my email and ensure its deliverability.

### The Flesch Grade Level Test

Emails are written with a characteristic grade level, and usually that grade level stays consistent across a category of

writing. As a simple example, stories in USA Today average a 10th grade level, while those in the Los Angeles Times average a 12th grade level (reference: <http://www.impact-information.com/impactinfo/newsletter/plwork15.htm>).

This same pattern holds true across given vendors and classes of emails &ndash; given a cursory investigation, emails from my bank appear to evaluate at around the 8th grade level, while sales emails from tech vendors evaluated around 7th grade level.

If you're trying to impersonate an email from Oracle, it's important that you're not writing at a similar level as a Ph.D. thesis. Luckily, you can use the Flesch Grade Level test (link: <http://www.addedbytes.com/lab/readability-score/>) to evaluate your emails against examples of emails you're trying to sound similar to.