



6 Simple Steps to Beat Phishing

Johannes Ullrich, SANS Internet Storm Center

Everybody knows about phishing. Phishers impersonate a trusted web site, commonly a bank or an online payment provider, in order to extract confidential information from users. Not only unsuspecting consumers are the victims of these scams, but in addition, the impersonated web sites will be impacted by reduced consumer confidence into their product, as well as by financial losses due to the misuse of the collected information.

This paper outlines some basic techniques that can be used to detect and avoid phishing schemes. These techniques can be considered due diligence for web sites commonly targeted by phishers.

1. Consistent Branding.

For a consumer, the first and sometimes only way to tell if a web site or an e-mail is trustworthy is the fact that either the URL or the layout "doesn't look right". In this context, it is important to provide consistent visual queues to end users to recognize communications from your business.

In particular e-mail sent to customers should use the same 'From' domain name as you use at your website. If you outsource mass mailings, insist that these e-mails will still use the familiar 'From' address. Consumers will otherwise not be able to distinguish between obvious fakes and real e-mail.

Assist customers in securing their systems by not requiring the use of Javascript and Active-X. In particular, design your web site to be accessible by various browsers.

2. Monitor bounces to customer facing e-mail addresses.

In order to advertise their fake web sites, phishers typically use the same methods and address lists used for spam. Many of the e-mail addresses on these lists are expected to be invalid. If you use consistent 'From' addresses (as proposed in (1)), the phisher will have to use this address to maximize success. This will result in some bounces being sent back to your own mail servers. Setting up a process to screen these bounces for phishing e-mail will provide an early warning mechanism to alert you of phishing scams.

3. Monitor referrers to public web sites.

Phishers typically redirect the user to the authentic web site after the information has been collected. This is done to hide the phishing site from the user and to improve its plausibility. The web browser will send the URL of the phishing web site as part of its 'Referrer' header. Web servers can be

configured to log this data, and most web servers already do so by default. Monitoring this log for unusual referrers will again assist in finding phishing web sites.

4. *Watermark web content.*

Phishers attempt to emulate the look and feel of your web site as good as they can. Typically, the HTML code and images from your site are just copied. As a result, the phisher will have to visit the authentic site before setting up the fake site. Encoding the IP address and a time stamp as part of your HTML code will likely allow you to figure out when the code was copied from your site, and who copied it. There are a numerous ways to accomplish this. Adding spaces between HTML tags, including extra GET parameters, or even watermarking images. The most appropriate method will depend on your web infrastructure.

5. *Preposition countermeasures*

Once you find a site impersonating you, there are a number of techniques you can use to limit damage. Most web servers will allow you to redirect users to special pages based on the referrer field sent by the browser. As phishing victims are frequently directed back to your site after they visited the fake site, you can use this technique to identify victims, or redirect them to a warning page. If they are existing customers of yours, you may be able to identify them based on prior cookies left behind by your site.

These countermeasures typically need to be prepared ahead of the phishing scam in order to evaluate the impact on web site performance. Once prepositioned, these redirects or special logs can be enabled quickly once a phishing site has been identified.

6. *Organizational and Administrative Countermeasures*

The company web site should include a link and contact information to report phishing or other security issues. All phishing countermeasures should be coordinated by a single individual.

Educating your customers about phishing, and showcasing samples for them to learn how to spot a phishing scam, will prevent them from becoming victims. If your web site allows access to critical financial or personal information (e.g. Banks, Brokerages), you should consider the use of strong authentication via hardware tokens.

It will decrease your response time, to discuss legal implications ahead of time and to have a legal response laid out ahead of time (e.g. letter drafted to be sent to ISPs in order to shut down impostor websites).

thanks to all the input from our handlers! This document will be made available exclusively at the SANS Internet Storm Center (<http://isc.sans.org>) and in the SANS Reading Room (<http://www.sans.org/rr>). For reprint and reuse permissions, please contact isc@sans.org