

Customer Advocate: Phishing Perspectives
infectionvectors.com
December 2005

Overview

Although banks have had to fight phishers for years already with public warnings, home page alerts, and press releases, there are many organizations that have yet to offer this service to their customers. As mentioned in many infectionvectors.com reports, every web-based organization is potentially the victim of scam artists on the Internet. More specifically, the customers of these companies are daily targets of phishing attempts. Protecting these customers should be an important (and not necessarily costly) goal. This report steps through the reasons why a company may find its customers the victims of a scammer and possible ways to protect those patrons.

Go Where the Crowd Is

Using simple, proven methods for duplicating web sites and drawing their own visitors, phishers have capitalized on the success of the refund-checking program. Below is an example of such a scam:

The IRS “Where’s My Refund” offering has been very successful, drawing in millions of visitors interested in checking the status of their US Federal Income Tax refunds. The IRS has offered the service since 2002 and has seen a steady increase in traffic since that time. Given the nature of the information requested and the authentication required, it also makes a good homestead for scam artists.

The scam above takes advantage of the basic trust most people have in official-looking documents. There are no glaring spelling or grammatical errors since the text is copied directly from the real IRS site, as is the logo. In fact, the entire website that acts as the net for unsuspecting refund seekers is copied from the actual irs.gov site (the scammers appear to have used a piece of freeware called HTTrack Website Copier, a useful tool for browsing websites offline, it could also be used to retrieve phony websites to see how they operate as well).

The email message does make one mistake: going to far in what it requests of the reader. From the text of the email:

```
To get to your refund status, you'll need to provide the following
information as shown on your return:</p>
```

```
<ul>
```

```
  <li>Your first and last name</li>
```

```
  <li>Your Social Security Number (or IRS Individual Taxpayer
Identification
```

```
Number)</li>
```

```
  <li>Your Credit Card Information <br>
```

Asking for credit card information is outside the scope of the actual program, and should set off a few warnings to moderately savvy readers. The link in the email (disguised as “Where’s My Refund?”) leads one to:

```
http://www.comunidadcristianaintl.org/libreriacci/catalog/images/.www4.
irs.gov/index.html
```

Not the IRS. The site posted to this address (the domain is registered to a location in Mexico) looks just like the IRS site, with the exception of the additional data requests mentioned above.

Spark

Any web-based service and any web-based company is the potential subject of a phishing attempts. If the service is very popular or has had a great deal of attention given to it, that potential rises exponentially.

That was the case with the IRS’ service, which was already growing in popularity when they announced that millions of dollars (US) in refunds were still outstanding in the second half of 2005. As the media picked up this story it no doubt piqued the interest of various scam artists, all planning another round of IRS-based phishing attempts.

Consumer Watchdog

The IRS combats the scam in a number of ways, and although they have numerous enforcement and investigative resources available to them, their strategy can help other smaller organizations. Their efforts, although far from perfect, can be scaled appropriately to meet the needs of any size consumer base.

First and foremost, they are on the lookout for scams which are targeted at their customers. Every organization has a client base; a subset of the population that is inclined to seek their services. Protecting this customer base is a priority for some organizations, and an afterthought of others. This is not meant to be a business administration lecture, but take a moment to consider where your organization falls on this matter. Keeping up with phishing attempts does not require a tremendous investment, there are sites dedicated to all areas of email/web scams already that can serve as the basis for this research. In addition, searching for your company or institution's name and/or domain name in anti-phishing newsgroups can be especially enlightening.

Second, the IRS maintains a "Fraud Alert" portal, where their research is meshed with tips to help unwary customers safe. This is also common for financial institutions such as credit card companies and banks, who have seen the need to protect customers or face an erosion of web-based commerce altogether.

Third, the IRS has made an attempt to take their warnings public, in a media-friendly and easily digested fashion. They issue a "Dirty Dozen" report every year which details the top scam attempts targeted at IRS customers. This effort is easily replicated for any type of business and can be housed along with general warnings on "public safety" page.

Never Ending Fight

Most web-based businesses have instituted privacy policies when if they collect personal information of any kind. That policy is almost universally linked from the company home page. Security information affecting customers (such as phishing warnings) should appear on the front page as well. In the case of the IRS, checking in the days prior to the publication of this report (20 December 2005) found no such warnings, surprising considering the apparent level of effort in stopping criminals from exploiting their customers.

Abandoning email for personal information requests has become the norm for companies with a web presence (and those without). Although it is an unfortunate loss in the battle against Internet criminals, there is simply no standardized means of guaranteeing the security of such messages. If this is not the policy of one's company, phishers will undoubtedly use email to pinpoint that company's clients.

Fighting scammers is a tricky business on its own; make no mistake about it. The prospect of investing a lot of funds into an education infrastructure is enough to turn

many businesses away from the Web altogether. Moreover, the automated, low cost HTTP/SMTP world is more than slightly dinged by the reality that email cannot be used to warn customers about email scams, as the entire medium has been reduced to an untrusted status. Education must be done as customers are visiting the site for the first time, and then on subsequent visits. That doesn't mean a 20-minute course for every shopping trip, just a link/banner here and there to keep security in the minds of clients. It means keeping on top of existing scams and reporting them to law enforcement, your own home page, and public relations department. Customer advocates are important pieces of the corporate and public sector structure; it is a job that is soon to be critical for all web-based institutions.

References

“IRS: Where’s My Refund Service Up Sharply.” 5 March 2004 SmartPros.

<http://www.pro2net.com/x42785.xml>

“IRS Announces the 2005 Dirty Dozen.” IR-2005-19, 28 February 2005.

<http://www.irs.gov/newsroom/article/0,,id=136337,00.html>

Search single groups or simply search all the newsgroups: <http://groups.google.com/>

IRS Tax Fraud Alerts Page

<http://www.irs.gov/compliance/enforcement/article/0,,id=121259,00.html>