

A hurricane strikes the coast leaving behind millions of dollars worth of damage and thousands of homeless people. You wish you could do something to help. Then you check your email, there in your inbox is a request for donations through a well-known, reputable charity. A picture of a family in front of their demolished home stares back at you as you type in your credit card number. The hurricane was real but the charity was impersonated.

You've been phished.

You polish your resume and post it on a leading career site. As you hold your breath waiting for an interview, checking your email frequently.

In your inbox is an amazing offer for an new suit from your favorite clothing company, it says the deal is given as a thank you to those who signed up for the career site you just joined. You click the embedded link to check out the offer. You recognize the clothing company's logo and slogan, it looks just like the site you've visited time and time again, so you browse through a handful of suits before you enter the color, style and size you want. Then you punch in your credit card number. You never receive the suit because you didn't visit the website of your favorite clothing company.

The website was pharmed and you've been phished.

You work for a major online retailer and take pride in the fact that your company was one of the first sites to offer secure purchasing transactions. Your organization has been encrypting credit card numbers for years, so you feel sure that your customers will never experience online fraud through any transaction they have with you. Then you find out hundred of your clients have been scammed by making a purchase through your site.

It turns out that your organization's database was hacked and the criminals stole lots of information on your clients – names, mailing addresses, email addresses and dates of last purchases. But, you wonder how they managed to get encrypted credit card numbers from your network... they didn't. They emailed your customers an urgent message saying that there was a problem with the credit cards they used to order from your site and they need to reenter them. The criminal provided an imbedded link that took them to a web page that looked just like the payment page on your site.

The webpage was pharmed, your clients have been phished and your organization has a lot of clean up to do.

Banks and financial institutions are no longer the prime target of online scam artists; phishers are now casting their nets to less suspecting organizations like career and utility sites – even non-profit organizations. Because criminals are often more technically savvy than the clients and organizations they hit, many victims never see them coming. The less you and your clients know about phishing the more apt you are to become a victim.

Terms you can't afford not to know:

- **Phishing:** Fraudulent emails or Web pages that often include a legitimate company's logo or images that attempt to illegally obtain clients' confidential information.
- **Pharming:** Code that compromises user's computers and redirects them to fraudulent websites – even if users type in the correct URL.
- **Identity theft:** The act of impersonating another, by means of using the person's information, such as birth date, social security number, address, name or bank account information.

The information obtained from these crimes can be used to charge expenses to victims' accounts create new accounts in their name and use their personal and account information for other illegal purposes.

The Price You Pay When You Get Fished

Direct losses due to online fraud are estimated as high as **\$3.1 billion** in 2008 for businesses and consumers. But, measurable amounts of money aren't the only losses when your organization becomes a victim.

- **Labor Costs** – Typically, your customer service takes a blow as call and email volume increase causing the quality of customer service responses to suffer. Valuable resource may have to be dedicated to handling the processes of reporting online fraud.
- **Online Overload** – Your website can become vulnerable as increased traffic could potentially bring it down. Further, your clients may have difficulty determining if your site is authentic, which could also spur calls or emails to your customer support center.
- **Brand Loyalty** – The brand you worked so hard to build could be challenged. You could lose the trust of clients if they feel that your company hasn't done enough to protect them against online fraud.

Top Three Ways to Help Prevent Online Fraud

1) Education

The best defense is informed clients, educate your consumers on the warning signs and how to report suspected phishing. One way to do that is to dedicate a page on your website to online fraud. The page should be easy to find on your site and include a number to call if they suspect they've been victimized. Such a page is also a great place to remind you clients of the age-old saying, "If it's too good to be true then it probably is."

Make sure ALL of your employees understand what phishing, pharming and online fraud are and what your company does to prevent them. Also, make sure your front line/ customer service staff knows what to say to clients in the event of an attack. This can be accomplished through training sessions and/ or by having a script prepared. Also educate your upper management and make sure your PR team is ready to answer/ handle media inquiries.

2) Security

Email addresses are becoming increasingly more valuable; your clients expect you to protect their address as you would an account number or SSN. Let them know that security measures are in place to protect their personal or account information – including email addresses.

In the event of an attack it is imperative that your consumers know how diligently you work to protect their data. Anything that contains customer information should have an audit trail.

3) Preparation

With phishing attacks on the rise, it's best to assume that your organization will get hit. You can help soften the blow by creating a crisis plan **before** you become a victim. A good place to start is in drafting an email that you could send to your clients to warn them when you are attacked.

The Bottom Line

Phishing is a costly and complicated crime. The tactics are ever changing and get increasingly more sophisticated. Staying up to date on the latest ways other organizations have been victimized is important, but the best way to minimize your losses is to begin preparing today as though your company will be a target tomorrow.

Related Websites

Here are a few websites to provide additional information on the topic and provide associated examples.

www.FTC.org

www.fraudwatchinternational.com

www.antiphishing.org

www.suntrust.com/alert

ABOUT THE AUTHOR

Sundee Kapur is an email marketing veteran, working with eCommerce marketers across multiple industries – helping them enable technology and services to brand, personalize and speak to their customers more effectively.

Sundee has presented at the DMA, Shop.org, Net.Marketing, ACC and Panel of Peers. His case studies have been published in multiple magazines and he has led a monthly workshop on email marketing since 1999 and has been with NCR for nearly 20 years.

ENHANCED WHITEPAPER

Visit the blog; join one of our calls or workshops:



Daily blog includes articles and links on subjects and trends affecting multi-channel marketers – we published our 450th searchable post in January 2009.

Relevant Posts:

Search these titles on the Email Yogi Blog for more information

Protect your Data (December 2008)
Spear Phishing (December 2008)
Ways to Spot Fraud (December 2008)
Not Quite (September 2008)
The Personal Touch: What NOT to Do (December 2007)



Monthly call focused on current interests and trends affecting multi-channel marketing. Customers and friends are invited to attend or listen to the podcast following the event.



Regional workshop series and annual conference brings together eCommerce marketing professionals for interactive learning and networking. Sessions feature case studies, email reviews and the latest in multi-channel marketing.