GUIDE

Stop Phishing: A Guide to Protecting Your Web Site Against Phishing Scams

GeoTrust®

Stop Phishing: A Guide to Protecting Your Web Site Against Phishing Scams

Introduction

If you use the Internet or spend any time checking the news, chances are you've heard about phishing.

Scan the headlines and you'll see stories about the latest scam tricking online shoppers into giving up their credit card numbers.

Look up "phishing" on any popular search engine and you'll get hundreds of thousands of results.

Phishing scams—ploys that cybercriminals use to trick unsuspecting people into revealing sensitive information and steal their identities—are a serious problem around the world. In 2008, more than five million people fell victim to phishing in the United States alone, and those numbers are on the rise.[1]

Whether you have or haven't heard of phishing, did you realize that it can be a serious threat to your business? Since phishing came on the scene almost 14 years ago, the number of attacks—and their level of sophistication—have skyrocketed. Phishers are now targeting more companies in a broader range of industries than ever before. If you have a web site and do business online, you are probably at risk.

Fortunately, there is an effective way to help protect your customers, your company, and your brand from phishing: Internet security technology called Secure Sockets Layer (SSL). SSL security—and a more robust version of the technology called Extended Validation (EV) SSL—authenticates web sites and encrypts sensitive customer data during online transactions like credit card purchases. These are two crucial security measures that can help customers tell the difference between legitimate sites and fake sites designed to steal their information.

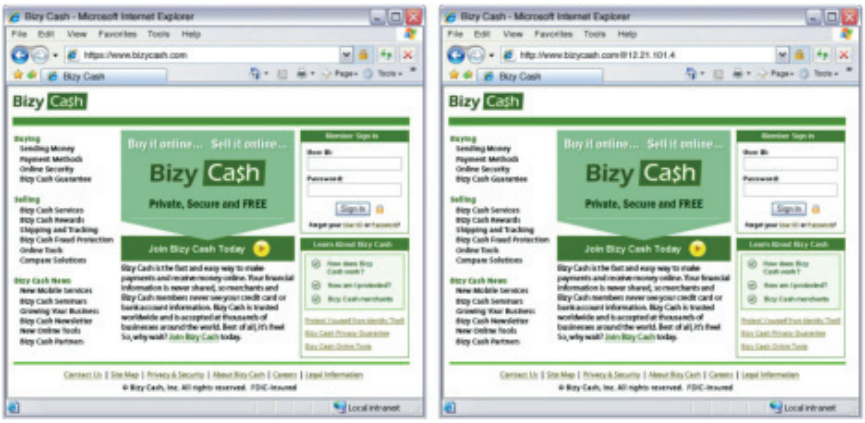
In this guide, you'll learn more about phishing, why it has become such a widespread problem, and the negative impact that a phishing attack can have on your company and your customers. You'll also learn how SSL and EV SSL technology can help protect your web site, your business, and ultimately your bottom line.

The Phenomenal Rise of Phishing

Imagine this scenario: You get an email from a prince or government official in Nigeria who promises you millions of dollars. All you have to do to get the money is send them your banking information so they can deposit the money into your account. Would you send them your information?

Of course not. In fact, you've probably heard of this particular scam before. The "Nigerian Letter" scam—also called a 419 scam in reference to the article of the Nigerian Criminal Code that prohibits fraud—is now an infamous phishing ploy. Up until recently, fake emails like these and other phishing attacks were fairly easy to spot. In addition to dubious claims about vast riches, many phishing emails came from strange addresses and directed recipients to web addresses with suspicious typos, all clear signs of phishing.

Today's phishers are much more sophisticated and have evolved far beyond simple emails. Phishers can now mimic legitimate sites much more effectively, making their malicious sites almost indistinguishable from the real thing. For example, a phisher might create a site that looks almost exactly like a bank web site, from the logo at the top of the page to the copyright information at the bottom.



One of these is a phishing site. Can you tell which one?[2]

The main difference? When users enter in their log in information, the data will be sent to the criminals who set up the phishing site. The phishers can then log into the accounts themselves and drain the users' funds, or sell the account information to other criminals trolling the underground market for identity theft information. Even worse, phishers are now targeting unsuspecting users through a variety of different channels, from email and web sites, to social media and mobile phones, and beyond.

With more avenues of attack, it should come as no surprise that the number of phishing scams is growing rapidly. The Anti-Phishing Working Group—a leading industry watchdog group—recently found online scam activity at an all-time high with more than 40,000 different phishing attacks being reported in the fourth quarter of 2009.[3] To underscore just how rapidly the problem has grown, Symantec discovered a 52 percent increase in phishing in the space of just one month.[4]

Spam and Phishing—A Recipe for Fraud

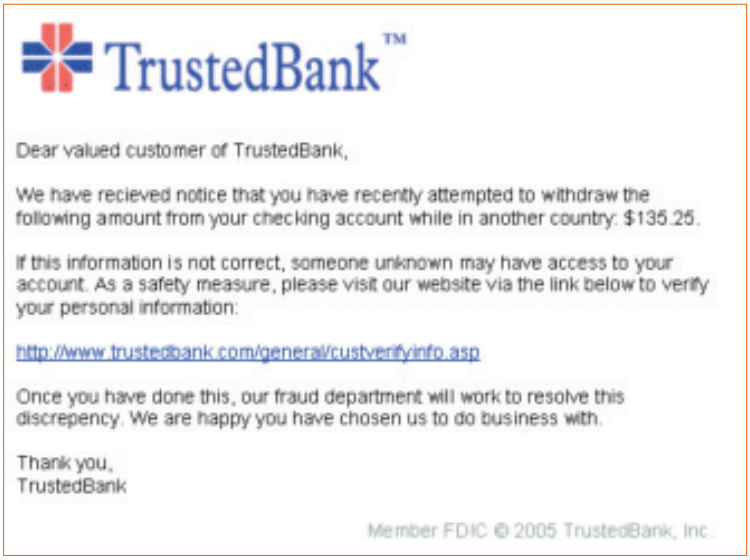
Spam is a favorite tool for phishers around the world, and one of the most effective ways that cybercriminals find new victims. If you use email, then you've probably heard of spam and you've almost certainly received a spam message. In fact, spam is estimated to make up more than 85 percent of all email traffic worldwide.[5]

Phishing and spam are closely related, but they're not the same thing. Simply put, spam is unsolicited bulk communications sent out over electronic messaging systems. Usually spam comes in the form of emails, but not always—spammers can also send out text message spam, instant message spam, and other types of mass messages.

Phishers create counterfeit emails and IMs to help drive traffic to their counterfeit web sites. These counterfeit messages become spam.

Not every spam message is a phishing message, but phishers often use spam to target their victims so it is safe to assume that a significant percentage of spam is tied to phishing. A spam phishing message may have the same noticeable giveaways that mark many phishing web sites—misspelled words, web site URLs that use a series of numbers rather than a company name, and other differences.

Spam is relatively inexpensive to send out, so phishers have to hook just a few victims to make their efforts worthwhile.



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

An example of a spam phishing email.

Socially Engineered Phishing Attacks

Just like legitimate retailers, phishers now use holidays, special events like back-to-school shopping, or other socially relevant occasions to entice users into falling for their schemes. For instance, cybercriminals exploited the popularity of the 2010 World Cup by spoofing online soccer gaming sites where they lured users into giving up their personal information with offers of free game software.[6]

How Phishing Hurts Customers—and Your Business

Since the financial industry deals closely with bank accounts and credit cards, it has been the primary target for phishers, but that doesn't mean it's the only industry that has come under attack. Phishers have set their sights on just about every type of organization, from ecommerce sites, to insurers, to government agencies, to telecom businesses, and even transportation companies. In fact, no business can be considered completely immune from a phishing scam.

Online consumers have learned this fact the hard way. It has been estimated that five percent of adults in the United States fall victim to phishing every year.[7] With about 250 million adults in the U.S., it's easy to see how the number of phishing victims can add up quickly.

Given the serious consequences of phishing and identity theft, it's no surprise that consumers are increasingly concerned about online shopping, banking, and other web-based transactions that involve sensitive information. These concerns are even leading to changes in online behavior: A recent poll found that 63 percent of online shoppers didn't complete a purchase because of security concerns.[10] Over time, those incomplete sales can translate into a substantial amount of lost revenue. According to one estimate, the fear of identity theft caused retailers to miss out on as much as $21 billion in online sales in 2008.[11]

Aside from directly impacting your bottom line, phishing attacks can severely damage your business's brand and reputation. If a cybercriminal phishes your web site and tricks your

customers into divulging their personal information, it can lead to an immediate loss of confidence in your site. Even though the attack isn't your fault, those customers may never buy from you again, and they may tell their relatives and friends to stay away from your web site, too. Upset, angry customers may even describe their negative experience on a blog, Facebook, Twitter, Yelp or other widely read sites. Online word of mouth information such as this can travel instantly to thousands of people online, especially now that Google indexes social media for search results. And this is compounded by the fact that any reader of these posts has multiple ways to easily forward it to their friends and family (via share, email, retweet, etc).

Concerns about phishing have led many people to educate themselves about online security and safety. Many online consumers now look for clear signs that that a web site is legitimate, including small padlock icons, "https://" at the beginning of web site URLs, and most importantly, familiar site seals and other trust marks. On legitimate sites, these types of indicators are usually available only by using SSL certificates.

The High Cost of Phishing

Phishing is big business for cybercriminals. In fact, the average phishing victim loses about $350 per incident.[8] Not only that, but phishing victims also have to worry about identity theft, a potentially devastating crime. According to the Identity Theft Resource Center, it takes an average of 140 hours per victim to recover from a serious incident of identity theft, including the time it takes to close bank accounts, dispute fraudulent charges, and clear credit reports.[9]

How to Protect Your Business from Phishing

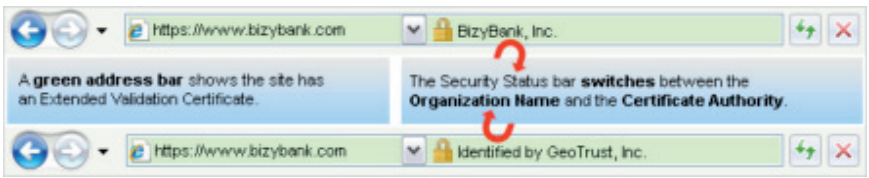
The sheer magnitude and sophistication of phishing scams—as well as the seriousness of their consequences—may seem overwhelming, but there are several best practices you can follow to help ensure that your business and your customers stay safe. One of the most important steps you can take is implementing SSL or EV SSL security on your web site. While you can use SSL to secure your web site, it is important to note that EV SSL offers stronger authentication and is clearly the best choice.

SSL Inspires Confidence

Customers look for signs of assurance that they are transacting with a legitimate web site. SSL can provide that assurance. When a web site is secured with SSL technology from a credible third-party provider, the company that owns the site must complete a validation process that confirms the business is legitimate. Usually, SSL providers will require companies to submit articles of incorporation, business licenses, or other types of proof. The SSL certificate itself—a snippet of code that enables private communication between a web site and a web server—encrypts sensitive customer data so hackers can't intercept it. Sites that are secured with SSL will display a small, clickable padlock icon, usually near or in the address bar, or in the lower right hand corner of the browser.

Extended Validation SSL Delivers Results

An Extended Validation (EV) SSL certificate will turn a web browser's address bar green in high-security browsers, giving customers tangible, highly visible proof that a web site is secure. The address bar will also display the name of the web site's legitimate owner and SSL provider, another security feature that confirms the identity of the site and puts customers at ease. The highly visible signs of security displayed in the web browser With Extended Validation (EV) technology require a more rigorous validation process.



EV SSL offers the highest levels of authentication available today and the browser display it triggers makes a very obvious security statement to web site visitors. It has become very popular for web sites that depend on establishing trust with their customers to use EV SSL.

Phishers can mimic many web site features, but they cannot turn web browser address bars green or display an organization's name in that location. These critical differences are what make using SSL technology—and EV SSL certificates in particular—so effective in protecting your site and your customers from phishing.

Take Action to Protect Your Business from Phishing

If you think you're ready to take the next step and implement SSL on your web site to protect against phishing, here are the steps you should take:

1. Research SSL providers and select a company that's well-known and has a solid reputation for security.

2. Strongly consider choosing an EV SSL certificate: The green address bar is a surefire way to show your customers that your web site is secure and legitimate.

3. Select an SSL provider that offers a highly recognizable trust mark: Be sure to display your trust mark prominently (above the fold) on your site—it will only be effective if your visitors can see it.

4. Create a security policy that clearly delineates how you use customer information and post it on your web site.

5. Spend some time educating your visitors and customers about SSL security and, if you use EV SSL, the importance of the green address bar. Post on your site a quick explanation of what SSL security is and how it protects web sites. You can explain what phishing is and how the green bar can help them tell the difference between legitimate sites like yours and fake phishing sites.

   Feel free to use information from this guide, or incorporate your own research to fit the needs of your particular business. There are a wealth of good resources for educating customers about online threats and safety. **The Internet Security Threat Report** is a great place to start.

Conclusion

Phishing is a widespread problem that continues to get worse. Unsuspecting consumers who fall victim to phishing scams can end up losing significant amounts of money, as well as their peace of mind. For American companies, the fear and uncertainty surrounding online security leads to billions of dollars in lost revenue every year.

Your business doesn't have to become part of these statistics. By using SSL security from a reputable provider, you can prove that your site is legitimate and protect your customers' online transactions. EV SSL technology offers even stronger protection against fraud and, with the help of the green address bar, lets you send a clear message that your site is authentic and safe to use. To effectively stop phishing and safeguard your business, SSL security should be at the top of your list.

The Importance of Trust Marks

Many SSL providers will also provide a seal or other type of trust mark that you can post on your web site to give visitors another signal that your site is protected. However, not all trust marks are created equally. The most convincing seals are dynamic and interactive, displaying an active time stamp confirmation and the name of the company that is being authenticated. Seals like these allow customers to see with a quick glance that the site's security information is current. Interactive seals also allow a web visitor to click on them to see additional information about the authentication of the web site. Also keep in mind that some seals are more recognized and trusted than others, so be sure to do your research and select a credible, well-known SSL provider.

Not All SSL Is the Same

Choose your SSL from an established, reliable, and secure independent certificate authority. It should deliver at minimum 128-bit encryption and optimally 256-bit encryption. It should be issued from a globally-available root infrastructure using 2048-bit RSA keys or better. The SSL issuing authority should maintain industrial-strength data centers and disaster recovery sites optimized for data protection and availability. Your SSL certificate authority must have its authentication practices audited annually by a trusted third-party auditor such as KPMG, Deloitte & Touche, or Ernst & Young. GeoTrust meets all of these requirements.

SSL Products from GeoTrust

GeoTrust offers a range of reliable low-cost SSL certificates to meet your individual needs:

- **GeoTrust® True BusinessID with EV –** Get the credibility of a well-established SSL provider, the green address bar and a dynamic trust seal from GeoTrust at an affordable price
- **GeoTrust® True BusinessID –** Get name brand SSL that authenticates your business identity along with a dynamic trust seal at an affordable price
- **GeoTrust® True BusinessID Multi-Domain –** Secure multiple domains or UC environments and get the convenience of an online self-service SAN management capability
- **GeoTrust® True BusinessID Wildcard –** Protect unlimited subdomains with reliable SSL from a certificate who maintains a reliable, military-grade data center
- **GeoTrust® QuickSSL® Premium –** Get inexpensive basic SSL encryption from GeoTrust's fast and convenient issuing system
- **GeoTrust® Enterprise SSL –** Purchase SSL certificates in bulk and issue them on demand
-

Contact Us

www.GeoTrust.com

CORPORATE HEADQUARTERS
GeoTrust, Inc.
350 Ellis Street, Bldg. J
Mountain View, CA 94043-2202, USA
Toll Free +1-866-511-4141
Tel +1-650-426-5010
Fax +1-650-237-8871
enterprisesales@geotrust.com

EMEA SALES OFFICE
GeoTrust, Inc.
8th Floor Aldwych House
71-91 Aldwych
London, WC2B 4HN, United Kingdom
Tel +44.203.0240907
Fax +44.203.0240958
sales@geotrust.co.uk

APAC SALES OFFICE
GeoTrust, Inc.
134 Moray Street
South Melbourne VIC 3205
Australia
sales@geotrustaustralia.com

1. "Protection Against Pharming and Phishing Attacks," Easy Solutions, Inc., 2009: http://www.antiphishing.org/sponsors_technical_papers/easysol_wp_phishing_pharming.pdf
2. The site on the right is a phishing site.
3. "Phishing Activity Trends Report, 4th Quarter/2009,"Anti-Phishing Working Group, March 2010: http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf
4. "State of Spam & Phishing: A Monthly Report," Symantec, October 2010: http://www.symantec.com/content/en/us/enterprise/other_resources/b-state_of_spam_and_phishing_report_10-2010.en-us.pdf
5. Ibid.
6. "State of Spam & Phishing: A Monthly Report," Symantec, July 2010: http://www.symantec.com/content/en/us/enterprise/other_resources/b-state_of_spam_and_phishing_report_07-2010.en-us.pdf
7. The Anti-Phishing Group at Indiana University: http://www.indiana.edu/~phishing/?prot_public
8. "Protection Against Pharming and Phishing Attacks," Easy Solutions, Inc., 2009.
9. Identity Theft Resource Center: http://www.idtheftcenter.org/artman2/publish/m_press/Aftermath_2009.shtml
10. "Americans' Online Shopping Decisions Affected by Security Concerns, Poll Finds," National Cyber Security Alliance, November 17, 2009: http://staysafeonline.mediaroom.com/index.php?s=43&item=54
11. "Survey Finds Retailers Missed Out on $21 Billion in Sales in 2008 Due to Online Shopping Fears,"Javelin Strategy, March 17, 2009: https://www.javelinstrategy.com/news/778/222/Survey-Finds-Retailers-Missed-Out-on-21-Billion-in-Sales-in-2008-Due-to-Online-Shopping-Fears/d,pressRoomDetail/