How to Avoid Phishing Attacks

A guide to protecting your business, website and customers

Symantec Website Security™

As a small or medium business professional, chances are you've heard about phishing. Phishing scams—ploys that cybercriminals use to trick unsuspecting people into revealing sensitive information and steal their identities—are a serious problem for both consumers and business owners. In fact, over the last five years, there has been a steady increase in attacks targeting businesses with less than 250 employees, with 43 percent of all attacks targeted at small businesses in 2015.[1] But phishing attacks aren't only targeting businesses, they're also targeting employees in order to gain access to a business' sensitive data. The number of spear phishing campaigns targeting employees increased by 55 percent in 2015.[2]

43%

43% of all attacks targeted small businesses in 2015.[1]

Since phishing came on the scene almost 20 years ago, the number of attacks—and their level of sophistication—has skyrocketed. A recent report by the Anti-Phishing Working Group (APWG) found that the number of phishing websites detected grew by 250 percent between this year and last year.[3]

Why Small Businesses Are a Target for Phishing Hackers

Phishers are now targeting any size of company in a broader range of industries than ever before. Small businesses are targeted more often for a few key reasons. First, SMBs tend to underestimate their risk level and thus aren't as careful about security. SMBs also tend to have less security in place than large enterprises. According to a chief Symantec strategist, "Small businesses are a softer target. In phishing campaigns, for example, attackers try to make people change the account on record for paying people, but in a large business, they have strong payments processes and that won't get through."

In this guide, you'll learn more about phishing and the negative impact that a phishing attack can have on your company, your employees and your customers. You'll also learn what measures you can take to help maintain a secure and trustworthy website.

What Phishing Looks Like

Imagine a small business employee gets an "urgent" email from someone posing as the CEO/Owner asking for all of the company's current and former employee tax forms. It sounds like an ordinary request from a trusted person, and the email looks legitimate, yet a hacker is behind the whole thing.

The employee innocently sends along the requested info, giving the hacker personal information on all employees. A data breach has occurred all because of a simple spear phishing attack, and any of that information can be used for identity theft.

What Is Spear Phishing?

Spear phishing is a special type of phishing attack that is designed to target a specific person or group. For instance, a spear phishing attack might be addressed to a person individually, or make reference to a regional event they attended, or refer to an article they read on LinkedIn.

Up until recently, 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. But today's phishers have evolved far beyond simple emails. They can now create entire fake websites that are almost indistinguishable from the real thing. For example, a phisher might create a site that looks almost exactly like a bank website, from the logo at the top of the page to the copyright information at the bottom.

> "Small businesses are a softer target."

When users enter their login information on these fake sites, the data is sent to the criminals who set up the phishing site. The phishers can then log in to 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 new avenues like social media and mobile phones. With more ways to attack, the number of phishing scams is growing rapidly, especially for smaller businesses.

Consumers are increasingly concerned about online transactions that involve sensitive information.

How Phishers Use Spam

Spam is a favorite tool for phishers around the world and one of the most effective ways that cybercriminals find new victims. Spam is estimated to make up more than 86 percent of the world's email traffic, with about 400 billion spam messages sent a day.[4]

Phishing and spam are closely related, but they're not the same thing. Spam is unsolicited bulk communications sent out over electronic messaging systems. Usually spam comes in the form of emails. But spammers can also send text messages and instant messages.

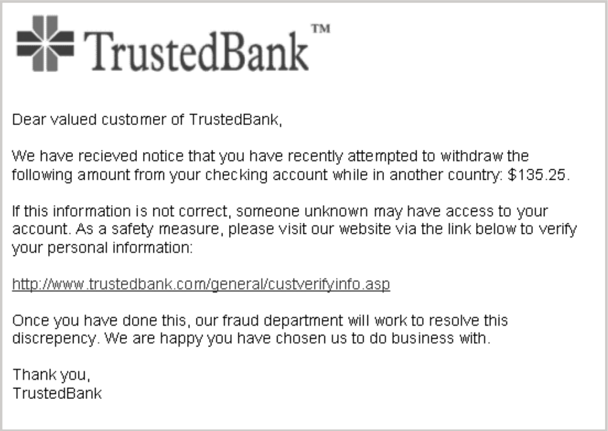
How to Spot a Phishing Email

Not every spam message is a phishing message, but phishers often use spam to target victims. So it's 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 websites, such as:

- Unofficial "from" address
- Urgent action required
- Link to a fake website or a URL that doesn't match the original website. Be sure to hover your mouse over any links embedded in emails.
- Website URLs that use a series of numbers rather than a company name
- Poor spelling or grammar
- Request for personal information

Educate Your Employees

Because phishers have so many tricks up their sleeves, you must ensure that your employees are aware of phishing and its dangers. If hackers gain access to your employees' information, they could then use that information to access your entire business' network. So establish a security policy that includes teaching employees about targeted hacking attacks sent via "fake" emails that look real, known as spear phishing attacks, so they can help protect their privacy and security, and yours too.



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

Figure 1: Example Phishing Email.

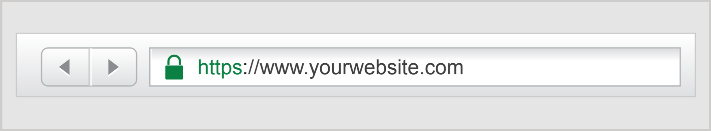
How Phishing Hurts Customers—and Your Business

No business is completely immune from phishing. Online consumers have learned this fact the hard way.

Given the serious consequences of phishing and identity theft, it's no surprise that consumers are increasingly concerned about online transactions that involve sensitive information. A recent poll found that 43 percent of respondents were worried about online security issues when shopping online.[5] If your site doesn't look reputable for any reason, a wary customer will simply leave and go elsewhere.

Because of more widespread awareness of online threats, many consumers now know to look for clear signs that a website is secure, such as small padlock icons, "https://" at the beginning of website URLs, and familiar site seals and other trust marks associated with an encrypted site that uses SSL/TLS security.

Showing consumers that a site is secure is such an important issue that many search engines are now starting to put SSL/TLS-encrypted sites higher in search ranking lists. Many browsers will now also mark unencrypted websites with a visual indication that the site is "Not Secure" to warn consumers to steer clear or beware that the site isn't safe enough.



https://www.yourwebsite.com

Figure 2: An example of an "https://" encrypted website

Build Customer Trust

Given that phishers can create sites that look legitimate, yet aren't, you must differentiate your website from those potential scam sites. You can do this by using two methods:

- Displaying a Trust Mark that the user can click on and validate its authenticity. The Norton Secured Seal displayed on a website allows the visitor to determine if it is a trustworthy site with a simple click.
- Using SSL/TLS certificates. SSL/TLS security—and a more robust version of the technology called Extended Validation (EV) SSL/TLS—authenticates websites and the business behind the website in addition to encrypting sensitive customer data.

Extended Validation SSL/TLS Delivers Results

An EV SSL/TLS certificate will display the name of the website's legitimate owner and SSL/TLS 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 EV technology require a more rigorous validation process. That's why using EV SSL/TLS has become very popular for websites that depend on establishing trust with their customers.

EV SSL/TLS offers the highest levels of authentication available today, and the browser display it triggers makes a very obvious security statement to website visitors. Phishers can mimic many website features, but they cannot display an organization's name when you click on the lock unless the site is encrypted with EV SSL/TLS. These critical differences are what make using SSL/TLS technology—and EV SSL/TLS certificates in particular—so effective in protecting your site and customers from phishing.

SSL/TLS and Trust Marks to Build Customer Trust

If you think you're ready to take the next step and implement SSL/TLS on your website to protect your customers and ensure they trust that your site is legitimate, here are the steps you should take:

1. Research SSL/TLS providers and select a company with a solid reputation for security.

2. Strongly consider choosing an EV SSL/TLS certificate due to the high assurance levels for end-users.

3. Select an SSL/TLS provider that offers a highly recognizable trust mark. Be sure to display your trust mark prominently and near fields that contain sensitive information on your site so your visitors can see it.

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

5. Spend some time educating your visitors and customers about SSL/TLS security. Post an explanation of what SSL/TLS security is and how it protects websites. Explain what phishing is and help them tell the difference between legitimate sites like yours and fake phishing sites.

Invest in Your Security

To build customer trust and protect your business, SSL/TLS security should be at the top of your list. While SSL/TLS does not stop phishing, it does give customers the sense of security they need to trust your site.

By using SSL/TLS security from a reputable provider like Symantec, you can prove to visitors that your website is legitimate and protect your customers' transactions. Your customers will find the Norton Trust Mark, see the "https://" logo, and know they are secure.

Why Choose Symantec?

- **Reputation:** When you choose Symantec, your site displays the Norton Secured Seal–the most recognized trust mark on the web, giving visitors confidence in your business and your site. Symantec displays over 1 billion trust seals daily.
- **Trustworthiness:** Symantec secures the world's top companies, including more than 90 percent of the Fortune 500, and is a longstanding, reputable market leader.[6]
- **Encryption and Beyond:** Symantec offers superior encryption that's 64,000 times stronger than industry standard (RSA) certificates, with daily malware scans, vulnerability assessments, warranty protection and installation tools to automate SSL Assist Plus.[7]
- **Authentication:** Multi-layered security makes our quick and easy certificate issuance and authentication processes the most rigorous in the industry.[8]
- **Expert Advisors:** We are present 24 hours a day, 7 days a week. Symantec continues to earn near-perfect scores for our customer service worldwide.[9]

To learn more about how Symantec website security can help you protect your website and your customers, contact us today.

To learn more, contact our sales advisors:

- **Via phone**
  U.S. toll-free: 1-866-893-6565
- **Visit our website at**
  www.symantec.com/ssl

[1] Symantec 2016 Internet Security Threat Report.

[2] https://www.symantec.com/content/dam/symantec/docs/infographics/istr-attackers-strike-large-business-en.pdf

[3] https://www.scmagazine.com/apwg-report-phishing-surges-by-250-percent-in-q1-2016/article/528186/

[4] https://www.bloomberg.com/news/articles/2016-01-19/e-mail-spam-goes-artisanal

[5] https://www.symantec-wss.com/campaigns/16557/assets/infographic/index-uk.html

[6] Internal customer analysis, October 2015 against Fortune 500 2015 list.

[7] NIST Special Publication 800-57 Part 1 Revision 4, "Recommendation for Key Management," January 2016.

[8] Symantec Global CSAT scores, April 2015 – July 2016.

[9] Symantec Global CSAT scores, April 2015 – July 2016.

For global offices and contact numbers, please visit our website.

For product information in the U.S., call:
1-866-893-6565 or 1-520-477-3111

Symantec World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com/ssl

For product information in Asia Pacific, call:
Australia: +61 3 9674 5500
New Zealand: +64 9 9127 201
Singapore: +65 6622 1638
Hong Kong: +852 30 114 683

Symantec Website Security Solutions Pty Ltd
3/437 St Kilda Road, Melbourne, 3004
ABN: 88 088 021 603
www.symantec.com/en/aa/ssl-certificates

For product information in the Americas (Non-U.S.), call:
Mexico: 554 738 0448
Brazil: 800 038 0598

For product information in the U.K., call:
0800 032 2101 or +44 (0) 208 6000 740

Symantec (UK) Limited
350 Brook Drive
Green Park, Reading
Berkshire, RG2 6UH UK
www.symantec.co.uk/ssl

For product information in Europe, call:
+353 1 793 9053 or +41 (0) 26 429 7929
Germany: 0800 128 1000
France: 0800 90 43 51
Spain: 900 93 1298

Follow Us:

Norton SECURED powered by Symantec

Symantec Website Security™