

## Phishing - How to Avoid Getting Caught

With so many of us online nowadays, it's inevitable that criminals familiar with computer technology have found ways to take advantage of it to make money. The Internet is almost impossible to police, as it crosses so many international borders, and criminals can operate basically from anywhere there's power and an internet connection. Phishing is just one of many schemes thought up by criminal minds to part us from our money.

Phishing is simply the scam of sending out a fake email in order to try and get the recipient to respond with private or financial information. You've probably received plenty of these - they pretend to come from a well known bank, tell you that someone has changed your password or that your account will be terminated if you don't confirm your details, and give you a link to click on.

Of course if you do actually click on the link, you'll be taken to a false website where the information you enter will be recorded and used to log in to your bank account or credit card and steal your money. In extreme cases, where the phishing attempt also gets private information such as your social security number, your whole identity may be stolen and used to apply for fake loans. Your financial and credit history can be ruined in literally hours, before you have any idea there's something wrong.

### How Do I Avoid Being Caught?

While this sounds terrible, there are things you can do to lessen the risk of your information being phished. The first, and most important, is to NEVER respond to an email that appears to come from your financial institution. It doesn't matter how legitimate it looks, or whether it has the right logos in it. These businesses are well aware of the rapid spread of phishing, and the last thing they would do is confuse things by sending an email requesting your login details or for you to confirm a password.

If in doubt, call your bank by looking up the phone number - don't use any phone numbers included in the email - and ask them if the email is legitimate. Never click on any links or URLs contained in the email, don't reply to the email, don't acknowledge that you've received it - just hit the delete button as fast as possible.

When you're visiting websites, always be wary of supplying too much private information. Only supply such information if you're sure it's a legitimate site that you've navigated to by yourself, and there should be a locked padlock logo in the bottom of the browser so you know the site is secure. Never enter this kind of information at a website you've reached by clicking on an email link.

### What Type of Phishing Emails Can I get?

Phishing isn't just limited to financial institutions. Many phishing scams imitate emails from eBay and well-known stores. They may appear to be a special offer, suggesting you click on the link to get a great deal on that particular item. The problem is that you'll end up at a website designed to steal your information, not the store's website. If you're especially interested in the deal being offered, call the store and ask if it's a genuine offer before clicking on anything.

If you do receive a suspicious email that you think is a phishing scam, it's always helpful to notify the company that it appears to come from. Some businesses have specific addresses for receiving phishing notifications, but many simply use postmaster@theirURL. PayPal can be reached via spoof@paypal.com. You can also report the scam to the Internet Crime Complaint Center, although this mainly deals with the more threatening and widespread phishing scams.

The important thing to remember is that you should never click on an email link without checking with your bank first. It doesn't matter how dire the consequences sound if you don't do it - that's all part of the scam. The more vigilant we all are, the less people will fall for phishing scams, and the better the chance that one day these criminals will give up and leave our inboxes alone.

Source: <http://www.articlecircle.com>

### About the Author

Steve Dolan is an IT professional with over 25 years experience in the industry. Find out how to protect yourself from phishing at <http://www.rspam.com/phishing> and avoiding spam at [www.rspam.com](http://www.rspam.com).