# E-Mail Phishing Examples

SecurIT360
*The physics of securing IT*

In a previous Overlook article, we covered tips for avoiding e-mail phishing attempts. This article will take a deeper dive into real-life e-mail phishing events which were successful and caused significant damage to the companies and people affected.

It is important to remember that even well-developed security programs can be brought down by a user who does not recognize a potential phishing attempt. Cyber criminals continue to improve their approach and the scenarios in which they attempt to trick e-mail users. However, training, awareness, and defensive habits can help you protect against most e-mail phishing activity.

## It Happens Millions of Times Every Day…

One of the most common e-mail phishing scams involves an e-mail which entices the user to click on a malicious link.

Unfortunately, this is a very successful method of e-mail phishing which has caused great financial damage, and in recent times, political damage.

This is the general premise. You receive an e-mail that looks like it is from a company that you do business with. It may be from your bank, Amazon, PayPal, eBay, Google, etc., and it has an alarming message like this.

> *"Your account has been compromised and you need to take action immediately."*
>
> *"Someone has your password and tried to login to your account."*

That would get anyone's attention, right?

It goes on to say –

> *"Click on the link below to change your password."*

## Don't Click the Link!

- Changing your password frequently is a good security practice.
- Changing your password when you suspect fraudulent activity on one of your accounts is a good security practice.
- Clicking on a link in an e-mail to change your password is a bad security practice.

If you receive an e-mail instructing you to click on a link in the e-mail to reset your password, you should:

- Close the e-mail.
- Open your internet browser or mobile phone application.
- Log in to your account.
- Change your password.

It is also a good idea to call the company and ask if there is a problem with your account. If they cannot confirm that your account was compromised, then you have probably been "phished".


© 2016 SecurIT360
dburns@securit360.com

# E-Mail Phishing Examples

SecurIT360
*The physics of securing IT*

## What's the Worst That Could Happen?

Some PayPal users could answer that question. A recent scam involved phishing e-mails that appeared to have come from PayPal. They used the PayPal logo, alerted the user that their account had been compromised, and instructed them to click on the link provided to change their password.

When the reader clicked on the link, it took them to a fake website, which was elaborately designed to look just like the PayPal website. The user was instructed to login and change their password. In reality, they just handed their PayPal user id and password to a cyber-criminal, who was then able to conduct transactions on their account.

This happens with banks, Amazon, and other companies. However, the majority of e-mail phishing attempts of this type involve PayPal or eBay accounts.

## How Did They Know I Had an Account with……?

We frequently see news stories stating that "XYZ Corp. had a data breach and two million records were stolen." Cyber-criminals horde information, and they are very patient. That is how they build databases of names, e-mails, account information and social security numbers to identify their targets. They gather information, plan their attack, and then send the e-mails.

It is safe to assume that some of the accounts that you use have been breached and that someone has information about you.

You should always change your password if you hear that a company that you do business with has been breached.

## The (Most Recent) Big One…

Perhaps the most famous recent phishing e-mail was sent to John Podesta, chairman of Hillary Clinton's presidential campaign. He received an e-mail which appeared to come from Google, instructing him to change his Gmail password. One of his aides asked their IT support if it was a legitimate e-mail. He replied that it was legitimate and that Podesta should change his e-mail password. However, instead of logging directly into his Gmail account, he clicked on the link…

This allowed hackers to easily access his e-mail account and expose thousands of e-mails to the public. It is difficult to measure the exact impact of this, but it certainly could not have been a positive thing.

It is important to note that using a very simple security practice might have completely avoided this monumental e-mail breach.

As always, develop a "cyber-defense" mindset and protect yourself.

If you would like to learn more about Cyber Security and how to protect your company, contact -

David Burns
Account Manager, SecurIT360
dburns@securit360.com
205.787.1250


© 2016 SecurIT360