



# DON'T GET HOOKED!

## WHAT IS PHISHING?

Phishing is a psychological attack used by cyber criminals to trick you into giving up information or taking an action. Phishing originally described email attacks that would steal your online username and password. However, the term has evolved and now refers to almost any message-based attack. These attacks begin with a cyber criminal sending a message pretending to be from someone or something you know, such as a friend, your bank or a well-known store.

These messages then entice you into taking an action, such as clicking on a malicious link, opening an infected attachment, or responding to a scam. Cyber criminals craft these convincing-looking emails and send them to millions of people around the world. The criminals do not know who will fall victim, they simply know that the more emails they send out, the more people they will have the opportunity to hack. In addition, cyber criminals are not limited to just email but will use other methods, such as instant messaging or social media posts.

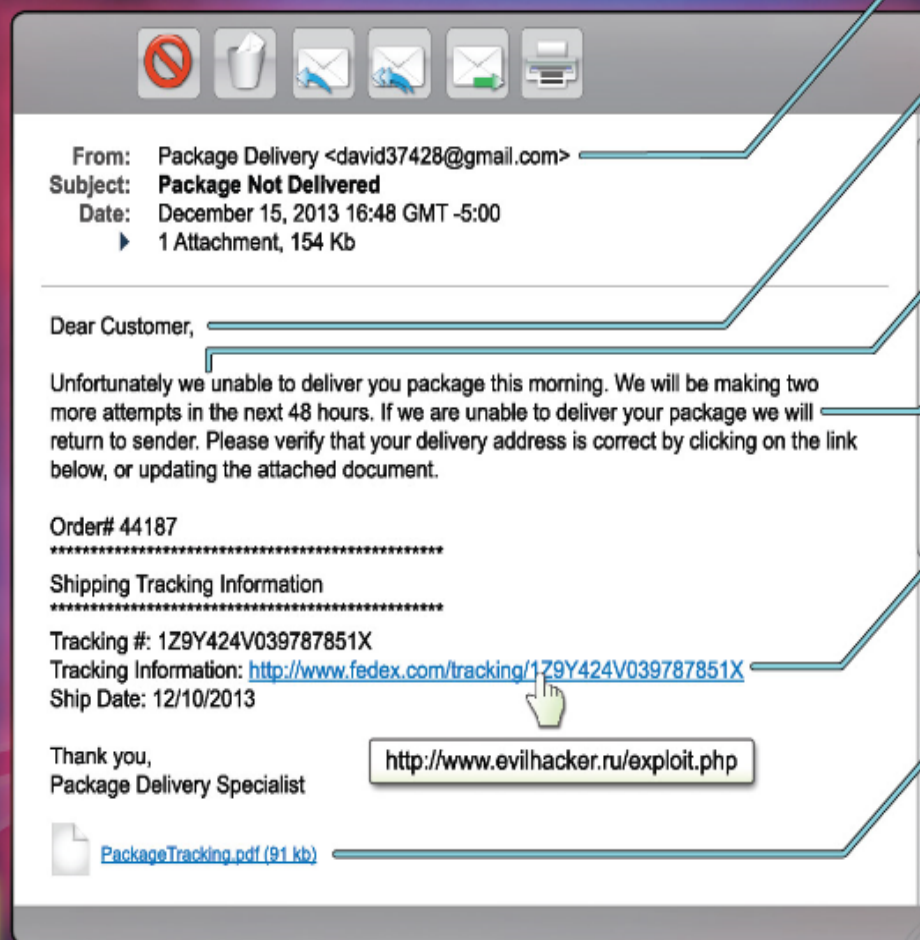
## WHAT IS SPEAR PHISHING?

The concept is the same as phishing, except that instead of sending random emails to millions of potential victims, cyber attackers send targeted messages to a very few select individuals. With spear phishing, the cyber attackers research their intended targets, such as by reading the intended victims' LinkedIn or Facebook accounts or any messages they posted on public blogs or forums. Based on this research, the attackers then create a highly customized email that appears relevant to the intended targets. This way, the individuals are far more likely to fall victim.

This poster was developed as a community project. Contributors include: Cheryl Conley (Lockheed Martin), Tim Harwood (BP), Tonia Dudley (Honeywell), Ellen Powers (MITRE Corporation), Shanah Johnson (Reserve Bank of Atlanta) and Terri Chihota.

## WHY SHOULD I CARE?

You may not realize it, but you are a phishing target at work and at home. You and your devices are worth a tremendous amount of money to cyber criminals, and they will do anything they can to hack them. YOU are the most effective way to detect and stop phishing. If you identify an email you think is a phishing attack, or you are concerned you may have fallen victim, contact your help desk or security team immediately. To learn more about phishing or to demo the SANS Securing The Human phishing testing platform, please visit <http://www.securingthehuman.org/phishing>.



## PHISHING INDICATORS

- A** Check the email addresses. If the email appears to come from a legitimate organization, but the "FROM" address is someone's personal account, such as @gmail.com or @hotmail.com, this is most likely an attack. Also, check the "TO" and "CC" fields. Is the email being sent to people you do not know or do not work with?
- B** Be suspicious of emails addressed to "Dear Customer" or that use some other generic salutation. If a trusted organization has a need to contact you, they should know your name and information. Also ask yourself, am I expecting an email from this company?
- C** Be suspicious of grammar or spelling mistakes; most businesses proofread their messages carefully before sending them.
- D** Be suspicious of any email that requires "immediate action" or creates a sense of urgency. This is a common technique to rush people into making a mistake. Also, legitimate organizations will not ask you for your personal information.
- E** Be careful with links, and only click on those that you are expecting. Also, hover your mouse over the link. This shows you the true destination of where you would go if you clicked on it. If the true destination is different than what is shown in the email, this is an indication of an attack.
- F** Be suspicious of attachments. Only click on those you are expecting.
- G** Be suspicious of any message that sounds too good to be true. (No, you did not just win the lottery.)
- H** Just because you got an email from your friend does not mean they sent it. Your friend's computer may have been infected or their account may be compromised. If you get a suspicious email from a trusted friend or colleague, call them on the phone.



# YOU ARE A TARGET

## Username & Passwords

Once hacked, cyber criminals can install programs on your computer that capture all your keystrokes, including your username and password. That information is used to log into your online accounts, such as:

- Your bank or financial accounts, where they can steal or transfer your money.
- Your iCloud, Google Drive, or Dropbox account where they can access all your sensitive data.
- Your Amazon, Walmart or other online shopping accounts where they can purchase goods in your name.
- Your UPS or FedEx accounts, where they ship stolen goods in your name.

## Email Harvesting

Once hacked, cyber criminals can read your email for information they can sell to others, such as:

- All the names, email addresses and phone numbers from your contact list.
- All of your personal or work email.

## Virtual Goods

Once hacked, cyber criminals can copy and steal any virtual goods you have and sell them to others, such as:

- Your online gaming characters, gaming goods or gaming currencies.
- Any software licenses, operating system license keys, or gaming licenses.

## Botnet

Once hacked, your computer can be connected to an entire network of hacked computers controlled by the cyber criminal. This network, called a botnet, can then be used for activities such as:

- Sending out spam to millions of people.
- Launching Denial of Service attacks.

You may not realize it, but you are a target for cyber criminals. Your computer, your mobile devices, your accounts and your information all have tremendous value. This poster demonstrates the many different ways cyber criminals can make money by hacking you. Fortunately, by taking some simple steps, you can help protect yourself and your family. To learn more, subscribe to OUCH!: a security newsletter designed to help people just like you.

[www.securingthehuman.org/ouch](http://www.securingthehuman.org/ouch)



## Identity Hijacking

Once hacked, cyber criminals can steal your online identity to commit fraud or sell your identity to others, such as:

- Your Facebook, Twitter or LinkedIn account.
- Your email accounts.
- Your Skype or other IM accounts.

## Web Server

Once hacked, cyber criminals can turn your computer into a web server, which they can use for the following:

- Hosting phishing websites to steal other people's usernames and passwords.
- Hosting attacking tools that will hack people's computers.
- Distributing child pornography, pirated videos or stolen music.

## Financial

Once hacked, cyber criminals can scan your system looking for valuable information, such as:

- Your credit card information.
- Your tax records and past filings.
- Your financial investments and retirement plans.

## Extortion

Once hacked, cyber criminals can take over your computer and demand money. They do this by:

- Taking pictures of you with your computer camera and demanding payment to destroy or not release the pictures.
- Encrypting all the data on your computer and demanding payment to decrypt it.
- Tracking all websites you visit and threatening to publish them.

This poster is based on the original work of Brian Krebs. You can learn more about cyber criminals at his blog at <http://krebsonsecurity.com>