



WelcomeSecurity
Enabling value through IT security

Phishing Attacks

Behind the scenes



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.

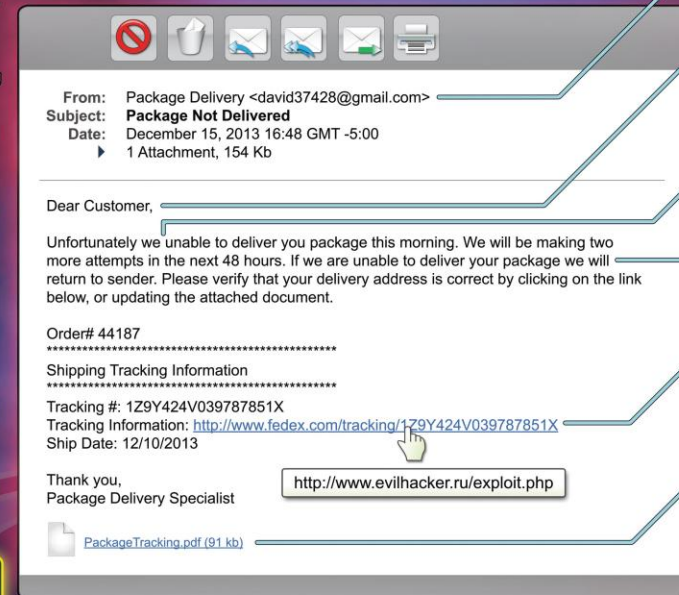
WHAT IS SPEAR PHISHING?

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 then 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.

© SANS Institute - You are free to print, distribute and post as many copies of this poster as you like, the only limitation is you cannot modify or sell it. For digital copies of this and other security awareness posters, visit www.securingthehuman.org/resources/posters

<https://www.sans.org/blog/new-security-awareness-poster-dont-get-hooked/>

Demo

Phishing

Fra: Info Nets <noreply@nets.com>
Dato: 8. marts 2017 kl. 10.07.57 CET
Til:
Emne: Adgang Til Dine Konto

Kære kunde Nets,

Det ser ud til, at en anden bruger din konto.

For din sikkerhed, har vi blokeret din konto
Vi har brug for nogle oplysninger for at løse dette problem

> Klik her <https://www.nets.eu/dk-da/l%C3%B8sninger/dankort/022136f>

© Nets i Danmark (HQ)-kontoteamet



Du har uforløste pakken

Vi har modtaget din pakke CT5389919582DK på 2015/09/21. Courier var ude af stand til at levere denne pakke til dig

Få og udskrive forsendelsesetiketten, og vise det på det nærmeste posthus for at få din pakke.

Få en adresselapp

Hvis pakken ikke er modtaget inden 20 arbejdsdage PostNord AB vil være berettiget til at kræve kompensation fra dig - 55 kroner for hver dag i at holde. Du kan finde oplysninger om fremgangsmåden ved og betingelserne af pakken holde i det nærmeste kontor.

Dette er en automatisk genereret meddelelse. Klik her for at afmelde

Fra: Skat.dk <skat@skat.dk>
Dato: 1. okt. 2013 12.00
Emne: ID:38933 - tilbagebetaling af skat - DKK 6940,00
Til: XXX



SKAT

Bemærk: Tilbagebetaling af skat for året 2012

Kære skatteyder,

Vores registreringer viser, at du er kvalificeret til en tilbagebetaling af skat af:
DKK 6940,00

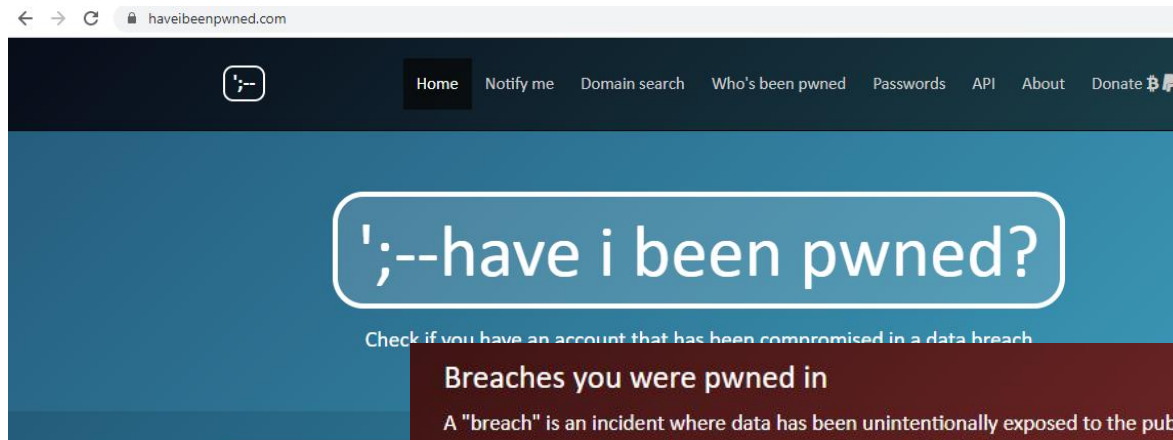
For at få adgang til din skat tilbagebetaling, klik venligst her.

Udfyld venligst formularen indtil d. 02-10-2013.

Den hurtigste og nemmeste måde at modtage din tilbagebetaling på er ved direkte inc
check/opsparingskonto.

Vores hovedkontor adresse kan findes på vores hjemmeside på
<http://www.skat.dk>

Copyright © 2013 Skat.dk. Alle Rettigheder Forbeholdes.



Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the [1Password password manager](#) helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



Data Enrichment Exposure From PDL Customer: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles



LinkedIn: In May 2016, [LinkedIn had 164 million email addresses and passwords exposed](#). Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords



Verifications.io: In February 2019, the email address validation service [verifications.io](#) suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an [archived copy](#) remains viewable.

Compromised data: Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses,

<https://haveibeenpwned.com/>



Backup for the demo

linkedin.com

microsoft.com

aws

Search [Alt+S]

Frankfurt

OWASP

Amazon SES

Configuration: Identities

Amazon SES

Get set up

Account dashboard

Reputation metrics

SMTP settings

Configuration

Identities [New](#)

Configuration sets

Dedicated IPs

Email templates

Suppression list

Cross-account notifications

Search all identities

	Identity	Identity type	Identity status
<input type="checkbox"/>		Domain	Verified
<input type="checkbox"/>	hack3r.party	Domain	Verified
<input type="checkbox"/>		Domain	Verified
<input type="checkbox"/>	xn--linkedn-0w4c.com	Domain	Verified
<input type="checkbox"/>	xn--mcrosoft-g80d.com	Domain	Verified
<input type="checkbox"/>		Domain	Verified
<input type="checkbox"/>	hacker@hack3r.party	Email address	Verified

On Tue, Dec 3, 2024 at 11:58 AM Amazon Web Services <no-reply-aws@amazon.com> wrote:

Hello,

Thank you for submitting your request to increase your sending limits. Your new sending quota is 50,000 messages per day. Your maximum send rate is now 14 messages per second. We have also moved your account out of the Amazon SES sandbox.

This takes effect immediately in the Europe (Frankfurt) region. You can view the current sending rate and sending quota for your account on the Sending Statistics page of the Amazon SES console, or by using the GetSendQuota API.

Phishing Email Template

Subject: Action Required: Unusual Sign-In Activity Detected on Your Microsoft Account

From: account-security@microsoft.com

Reply-To: noreply@microsoft.com


Body:

Dear [Name],

We detected unusual sign-in activity on your Microsoft account [yourname@ft.fo] from an unrecognized device or location. For your security, we have temporarily locked access to your account.

Message ChatGPT

Action Required: Unusual Sign-In Activity Detected on Yo...

 Summarize



account-security@microsoft.com

To  Thomas Ljungberg Kristensen - WelcomeSecurity



08.02



If there are problems with how this message is displayed, click here to view it in a web browser.

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.



Dear Thomas,

We detected unusual sign-in activity on your Microsoft account **[thomas@welcomesecurity.net]** from an unrecognized device or location. For your security, we have temporarily locked access to your account.

To restore access and verify that this activity was authorized, please confirm your account information by clicking the secure link below:

[Review Activity](#)

If you recognize this activity, you can safely ignore this message. However, if you fail to verify your account within **24 hours**, access to Microsoft services such as Outlook, Teams, and Azure DevOps may be restricted.

For assistance, contact our support team at **security-support@microsoft.com**.

Thank you for helping us keep your account secure.

Best regards,



WelcomeSecurity
Enabling value through IT security

Thanks!

Thomas Ljungberg Kristensen

www.welcomesecurity.net

+45 2158 1410

thomas@welcomesecurity.net

