

# THE DANGERS OF PHISHING: HELP EMPLOYEES AVOID THE LURE OF CYBERCRIME



# PHISHING

/ˈfɪʃɪŋ/

**noun**

**1. the practice of using fraudulent e-mails and copies of legitimate websites to extract financial data from computer users for purposes of theft<sup>1</sup>**

Phishing remains cybercriminals' method of choice to infect users' computers. Corporate employees are particularly vulnerable since they are heavily targeted as an easy entry into sensitive data.

Generally speaking, tricking users into giving up information is referred to as "social engineering." Given the need to be able to simultaneously go after hundreds or even thousands of users at once, attackers created a new method which we now refer to as "phishing."

This eBook will describe some typical phishing schemes, the evolution of phishing over the last few years, and tips for keeping your business safe.

## PHISHING 101

Phishing is the ultimate social engineering attack. Most of the original social engineering attacks were one-on-one attacks which were effective, but not scalable. Phishing gives a hacker scale and the ability to go after hundreds or thousands of users at once.

Phishing is a kind of malicious attack where cybercriminals create fake emails and websites—meant to look like a popular online resource (a social network, online banking services, or online games) and use various social engineering methods to attempt to lure users to the website. Typically, a phishing page contains text fields for users to enter their personal data.


The type of data of interest to the cybercriminals will ultimately determine the type of phishing attack. For example, if the malicious user's goal is to steal data in order to access a victim's social network account, then he will attempt to get users to give their email address and password to the social network using a fake website designed to look like the social network. Common social engineering methods used to infect users include sending messages with embedded URLs that redirect to phishing sites as well as sending phishing emails with malicious attachments that are rigged with exploits. The attackers' objective is gaining account credentials or personally identifiable information (PII), contact information, links to other accounts, which are used for monetary gain via identity or financial theft.

# THE EVOLUTION OF PHISHING

According to the "Anti-phishing Work Group's Q4 2013 Report," the number of phishing sites detected rose significantly in 2013, making it one of the most active years on record for this particular type of malicious attack:

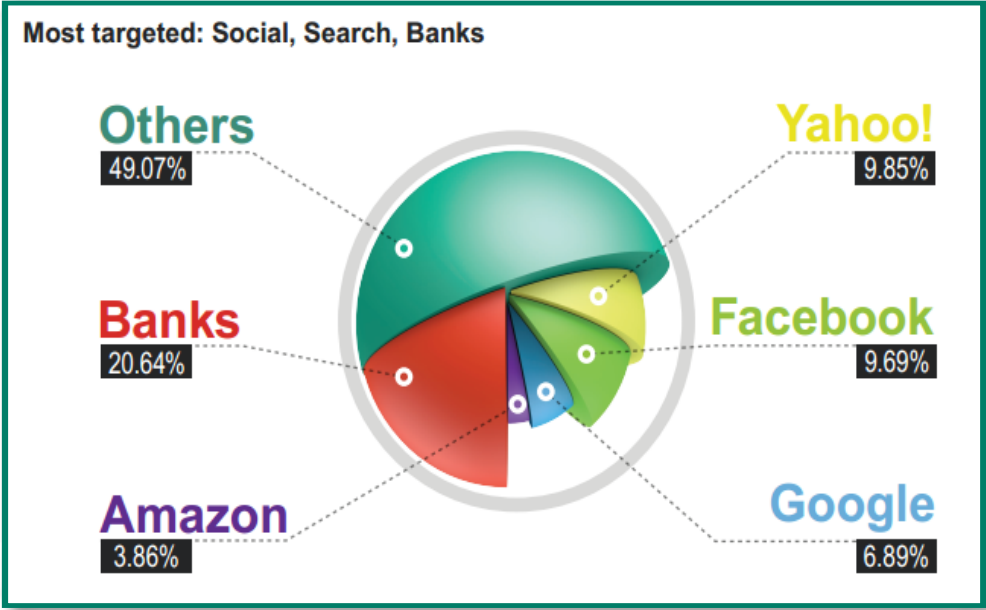
- In 2012-2013, 37.3 million users around the world were subjected to phishing attacks, up 87% from 2011-2012.<sup>2</sup>
- Over 20% of all attacks targeted banks and other credit and financial organizations which can have an impact on businesses in every industry.<sup>3</sup>
- 102,100 Internet users around the world were subjected to phishing attacks daily.<sup>4</sup>
- The U.S. continues to be the top country hosting phishing sites during the fourth quarter of 2013.<sup>5</sup>

Clearly, cybercriminals are more frequently resorting to phishing in an attempt to steal money or valuable financial information directly from users.

A silver laptop is open on a light-colored wooden desk. The laptop screen displays a white background with green text. The text reads: "In 2012-2013, 37.3 million users around the world were subjected to phishing attacks." The laptop is positioned in the lower right portion of the image, with a blurred background showing a window with natural light.

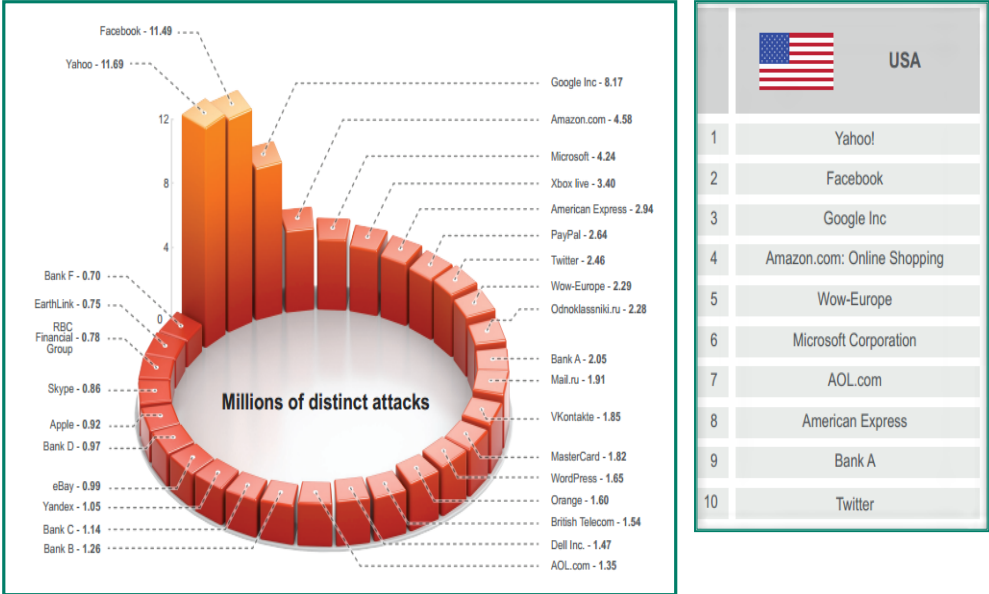
In 2012-2013,  
37.3 million users around  
the world were subjected  
to phishing attacks.

# PHISHING TARGETS



6

In addition to targeting business sites, cybercriminals focus on consumer sites used by business people during work hours.

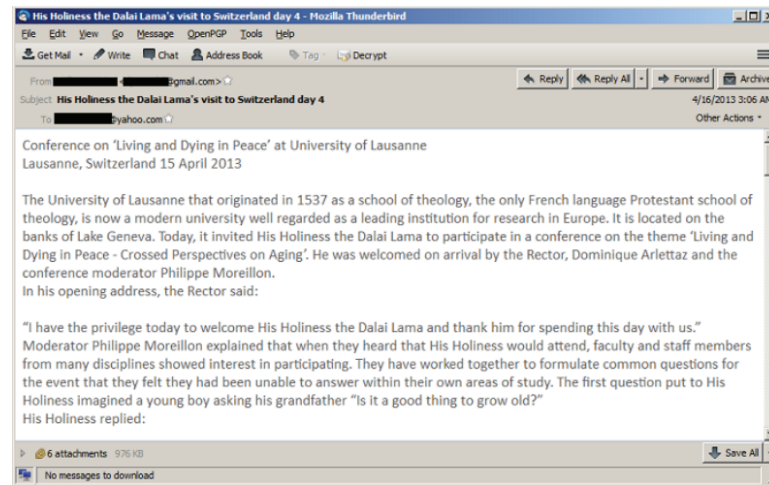


7

	 USA
1	Yahoo!
2	Facebook
3	Google Inc
4	Amazon.com: Online Shopping
5	Wow-Europe
6	Microsoft Corporation
7	AOL.com
8	American Express
9	Bank A
10	Twitter

Cybercriminals are using online storefronts and banks to get user's credentials and then use those credentials to infiltrate the employer's network, putting your business at risk.

# DALAI LAMA PHISHING EXAMPLE



Sometimes phishing schemes come in the form of targeted attacks. One recent example was a cyberespionage campaign called “NetTraveler,” analyzed by Kaspersky researchers in June 2014. Attackers sent a spearphishing email with text about the Dalai Lama visiting Switzerland to a number of activist groups. The email included multiple decoy images depicting a large Tibetan audience, and the Dalai Lama speaking.

The email included several malicious Word attachments exploiting known vulnerabilities – even though these have been patched by Microsoft® they’re still widely used in targeted attacks when trying to find victims with unpatched systems. Again, a dangerous combination of social engineering and common exploitable vulnerabilities. In this case, the attack happened in 2013 and exploited a vulnerability patched in 2010.

# TAKING IT UP A NOTCH

So what if all of the previous techniques don’t work? Attackers will then try something that is more focused and customized: spear-phishing and targeted attacks.

So-called “spearphishing” emails used in targeted attacks are one of the most common methods for infecting valuable targets in corporations.

According to the Global IT Security Risks Survey of 2014:

- 94% of companies surveyed had at least one external security incident.
- The estimated impact of a data breach on an enterprise-sized business rose by 14% to \$798,000.
- 87% of businesses that suffered data loss required additional professional services and 47% incurred significant additional costs.
- The typical damage of a breach (including the costs of hiring professional services, increased downtime and lost business opportunities) was \$35,000 for small-to-mid-sized business and \$690,000 for enterprises.<sup>9</sup>





# THE BIGGEST PROBLEM

1

In 2013, vulnerabilities in Oracle Java® accounted for more than 90% of all cyberattacks.<sup>10</sup>

2

More than 160 vulnerabilities were reported to Oracle by the IT security community.<sup>11</sup>

3

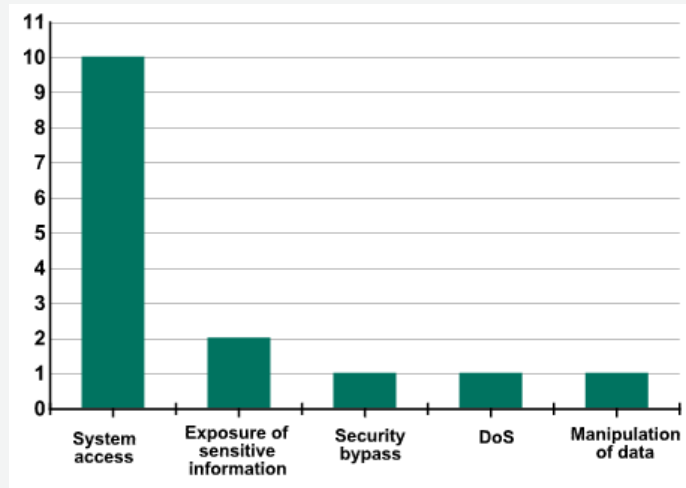
Kaspersky Lab detected more than 14.1 million Java-based attacks in 2013.<sup>12</sup>

4

Windows® components, Android™ and Adobe Acrobat Reader® accounted for the largest amount of remaining exploited vulnerabilities.



# EXPLOITING VULNERABILITIES



13

- Vulnerabilities enable attackers to execute malicious code or take full control of the system.
- Several exploits can be developed per vulnerability and are high commodities in the cybercriminal underground.

# IT MANAGER'S PHISHING PREVENTION TIPS

- Do not have a list of all employees on your company website.
- Regularly scan internet for exposed email addresses and/or credentials.
- Educate users about dangers of leaving too much information on social media sites.
- Practice simulated spearphishing attacks on employees to raise awareness.
- Keep your system and programs updated.
- Install (and use all the features of) a reliable security solution, including vulnerability scanning, patch management, and advanced malware detection.
- Users should be cautious and mindful of what websites they are accessing and what files they are opening on corporate computers and devices.
- They should be aware that they are working for a organization with data and information, that is a valuable commodity on the cybercriminal market.
- Everyone will probably face a targeted attack at least once in their career, and while attackers generally prefer executives, HR, and legal staff, they will try anyone.
- Attacks will most likely be more sophisticated in terms of social engineering.
- Emails could come from other employees or even top management.
- Users should always be vigilant, and when they are suspicious, they should examine emails carefully.

# SOPHISTICATED THREATS REQUIRE MULTI-LAYERED PROTECTION

Cybercriminals and the malware they create are evolving and changing on a daily basis and it's impossible to protect an organization if you aren't aware of the dangers. B2B International surveyed businesses and Kaspersky Lab analyzed the data in its most recent report, "IT Security Threats and Data Breaches." Released in 2014, the report revealed a major gap between perception and reality<sup>14</sup>:

- During 2013 and 2014, Kaspersky Lab detected around 315,000 daily malicious samples but only 4% of businesses surveyed were able to accurately state that figure.
- At the end of 2013, Kaspersky Lab researchers had detected 200,000 unique malware code samples. By the end of the first half of 2014, that number had increased to 375,000.

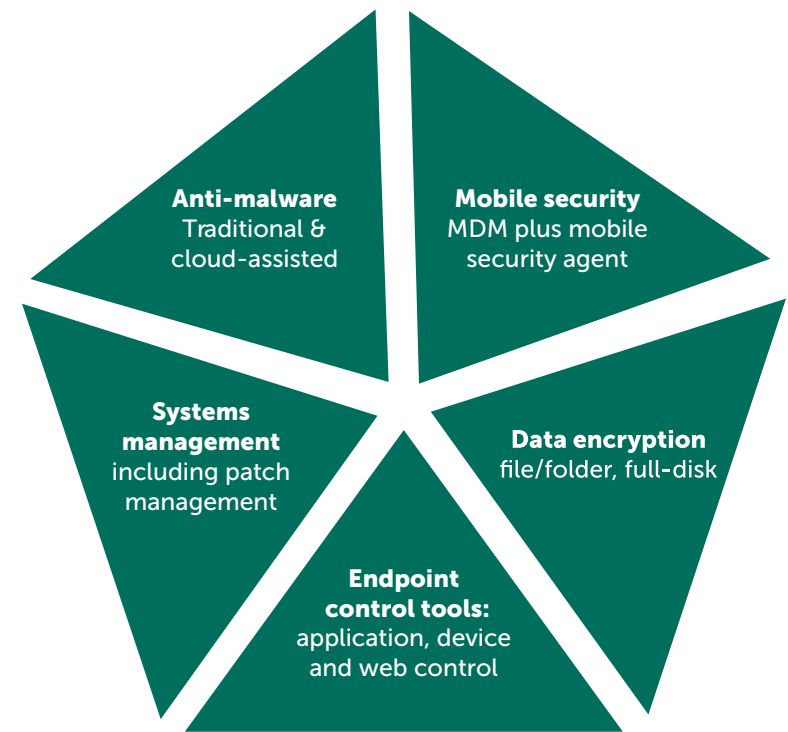
Simple steps like patch management can substantially decrease your vulnerability. The most actively exploited programs in targeted attacks are Microsoft Office®, Adobe Reader®, Adobe Flash®, Internet Explorer® and Oracle Java, so keeping software, operating systems and third-party applications updated should be a top priority.

For larger and more complex IT infrastructures patch implementation can take longer, which increases the risk of the publicized vulnerabilities being exploited. Consider using advanced protection technologies such as Automatic Exploit Prevention (AEP) which uses Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) mechanisms as methods of heuristic analysis and control over executable code to block the execution of malicious code before it's patched or when a zero-day vulnerability is being used.



# KASPERSKY SECURITY FOR BUSINESS

PHYSICAL » VIRTUAL » MOBILE »



Vulnerability Scan

Patch  
Management

Remote Tools

License Management

System Provisioning

(NAC) Network  
Admission Control

# SYSTEMS MANAGEMENT & ACTIONABLE PATCHING

## SYSTEM PROVISIONING

- Create images
- Store and update
- Deploy



## VULNERABILITY SCANNING

- HW and SW inventory
- Multiple vulnerability databases



## LICENSE MANAGEMENT

- Track usage
- Manage renewals
- Manage license compliance



## ADVANCED PATCHING

- Automated prioritization
- Reboot options



## REMOTE TOOLS

- Install applications
- Update applications
- Troubleshoot



## NETWORK ADMISSION CONTROL (NAC)

- Guest policy management
- Guest portal



# PROTECT YOUR BUSINESS NOW.

*Join the conversation.*



Watch us on  
YouTube



Like us on  
Facebook



Review  
our blog



Follow us  
on Twitter



Join us on  
LinkedIn

GET YOUR FREE TRIAL NOW >

Learn more at  
[kaspersky.com/business](https://kaspersky.com/business)

## ABOUT KASPERSKY LAB

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997 Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide.

**To learn more about Kaspersky Endpoint Security for Business, call Kaspersky Lab today at 866-563-3099 or email us at [corporatesales@kaspersky.com](mailto:corporatesales@kaspersky.com).**

[www.kaspersky.com/business](https://www.kaspersky.com/business)

© 2015 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.

**KASPERSKY**  
lab  
THE POWER  
OF PROTECTION