SECURITY SPOTLIGHT

The dangers of phishing:

help employees avoid the lure of cybercrime

KASPERSKY lab

Phishing scams are a form of cybercrime that involves defrauding users to obtain sensitive information. Cybercriminals act as legitimate companies or organizations to obtain the information.

Phishing

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.

Cybercriminals use social engineering to trick their victims into launching malicious files on their computers, opening a link to an infected website or or sending criminals their private data.

We'll take a look at typical phishing schemes, the evolution of phishing and tips for keeping your business safe.

Phishing 101

Phishing is the ultimate social engineering attack, giving a hacker the scale and ability to go after hundreds or even thousands of users all at once.

Phishing scams involve sending out emails or texts disguised as legitimate sources. They may look like they are from a trusted vendor or a law enforcement authority, but secretly, they contain malware. These messages are specifically designed to trick the victim into opening the email through the tactics of fear and intimidation. Once a person opens it, the malicious software downloads onto their computer, and the cybercriminal is in your system.

Common social engineering methods include sending messages with embedded URLs. Once the person clicks on the link, they are re-directed to a phishing site. A phishing email can be sent with a malicious attachment that is rigged with exploits, often with the claim that the attachment is an unpaid invoice that needs attention.

What it all comes down to is access, and your employees are the first line of defense. Even if you are a small company, if you serve a large enterprise, then you are a desirable target who can provide the portal that cybercriminals are looking for to get to the big payoff of accessing a multi-national corporation.

The evolution of phishing

The Anti-Phishing Working Group (APWG) observed more phishing attacks in the first quarter of 2016 than in any other three-month span since it began tracking data in 2004.[1]

There is no doubt that phishing continues to be a favorite method of cybercriminals:

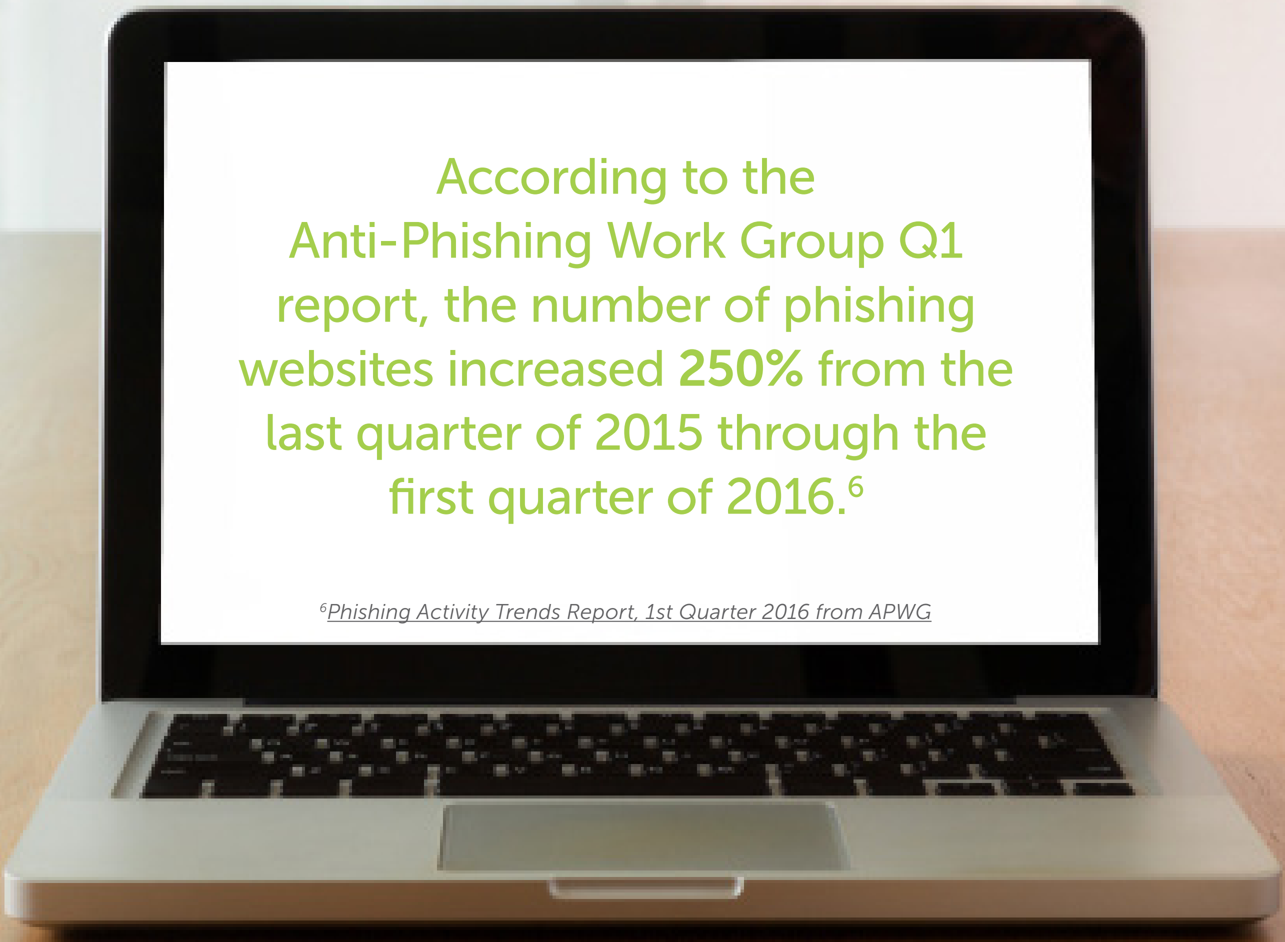
- 48.13% of all phishing attacks registered by Kaspersky Lab products were focused on gleaning users' financial data.[2]
- During Q4 2016, Kaspersky Lab registered attacks with financial malware against 319,692 users worldwide. That is 22.49% more than during the same period in 2015.[3]
- China (20.21%) remained the country where the largest percentage of users is affected by phishing attacks.[4]
- In Q3 2016, Kaspersky Lab products prevented over 37.5 million attempts to enter phishing sites, which is 5.2 million more than the previous quarter.[5]

Clearly, this is a problem that is not going away and, in fact, only continues to grow.

[1] *APWG report: Phishing surges by 250 percent in Q1 2016*

[2, 3] *Holiday 2016 financial cyberthreats overview*

[4, 5] *Spam and Phishing in Q3 2016*



According to the Anti-Phishing Work Group Q1 report, the number of phishing websites increased **250%** from the last quarter of 2015 through the first quarter of 2016.[6]

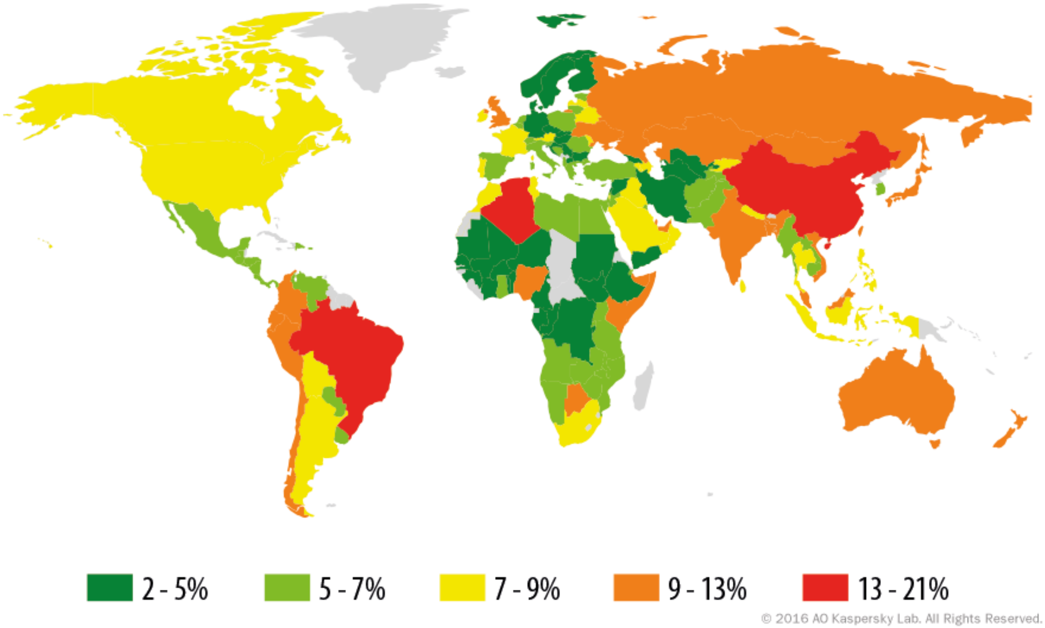
[6] Phishing Activity Trends Report, 1st Quarter 2016 from APWG

The Olympics in Brazil

For a number of years now, Brazil has been among the countries with the highest proportion of users targeted by phishing. In 2015 and 2016, phishers focused on the Rio Olympic Games in Brazil. Kaspersky Lab Q1 data showed that in addition to ordinary users, the potential victims of phishing included the organizers of the Olympic Games.

The Olympic theme remained popular in Q2 2016, with phishers working overtime to send out fake notifications about big cash wins in a lottery that was supposedly organized by the Brazilian government and the Olympic Committee.

Geography of phishing attacks*, Q2 2015

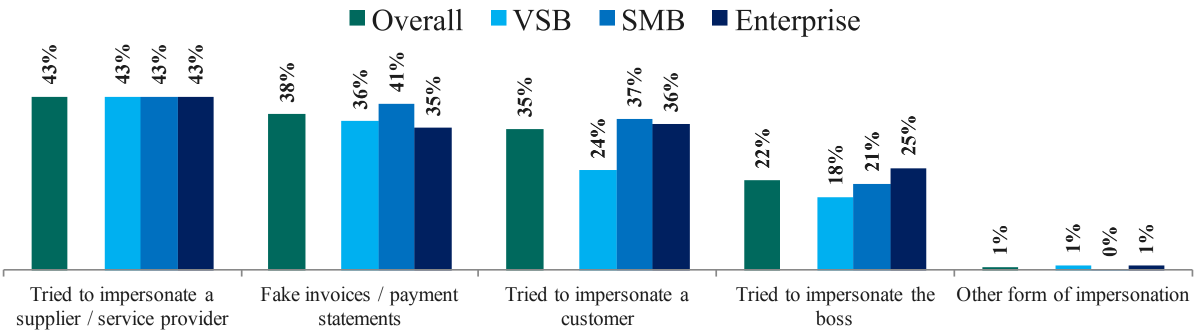


** Number of users on whose computers the Anti-Phishing system was triggered as a percentage of the total number of Kaspersky Lab users in the country*

Source for this visual: *Spam and Phishing in Q2 2016*

Phishing attacks

% Of Those Suffering From Phishing Attacks Targeted In Each Way



Smaller businesses are not worth targeting specifically so they tend to only receive generic phishing attempts impersonating service providers and submitting fake invoices/payments. Attempts against larger businesses can be far more tailored, impersonating customers or even senior staff.

Taking it up a notch

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.

Spearphishing attacks tend to target large enterprise organizations more, particularly the C-level staff. Smaller businesses are not seen to be worth targeting specifically, so they tend to only receive generic phishing emails that impersonate service providers or submit fake invoices. Attempts against larger businesses can be far more tailored, impersonating customers or even senior staff.

Top tips to protect your company from phishing

- 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 an 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.

A comprehensive phishing solution

How Kaspersky Lab’s Anti-Phishing Technology Works

The anti-phishing module implemented in Kaspersky Lab’s solutions provides effective protection against phishing schemes combining three methods of detection:

- Sites are checked by the product’s local anti-phishing databases on the user’s device;
- Sites are checked by cloud databases located on the Kaspersky Security Network;
- Heuristic analysis helps recognize a phishing webpage even if it’s not yet featured in these databases.

Keeping a Comprehensive Database of Phishing Sites

Kaspersky Lab maintains a vast, constantly updated, database of phishing sites. It accumulates information about all phishing pages received from a number of partners, as well as those detected by Kaspersky Lab’s technologies. Databases that contain harmful URLs are regularly sent to Kaspersky Lab’s solutions, as well as the cloud database (Kaspersky Security Network), which holds the most full and accurate collection of these. When a new malicious URL is detected on the computer, information about this threat is made available from the cloud database within 15-30 seconds of detection.

Determining Safe URLs

The same database of anti-phishing sites also strengthen the functionality of yet another technology. Information from this database, supplemented with data about other malicious sites, is being used by the Kaspersky URL Advisor reputation service. When someone uses one of the popular search engines, the URL Advisor checks the links that were found and marks them as either those that can be trusted or those that may lead to a phishing site.

This technology is indispensable for combating phishing, since attackers use all sorts of tricks to give credibility to their links: they publish them in the newsfeeds of compromised accounts on social networks, use various illegal SEO schemes to push fake pages to the top of search engine results for popular keywords, along with other tricks designed to escape notice.

A comprehensive phishing solution

Using the Last Line of Defense

The heuristics module is a user's last line of defense against a phishing attempt. It is a highly effective system that allows Kaspersky Lab to give a reliable verdict about whether a site encountered by the user is a phishing one or not, even if it is not listed in the local or cloud databases. According to Kaspersky Lab's statistics, almost 50% of phishing detections are made by this system.

Anti-phishing modules look at dozens of phishing symptoms, such as domain names, frame usage, and input encryption usage, and compare them with other indications. The heuristics module is an intelligence system that analyzes and classifies those indications based on the knowledge of known modern phishers' methods and the vast Kaspersky Lab database of already detected phishing sites.

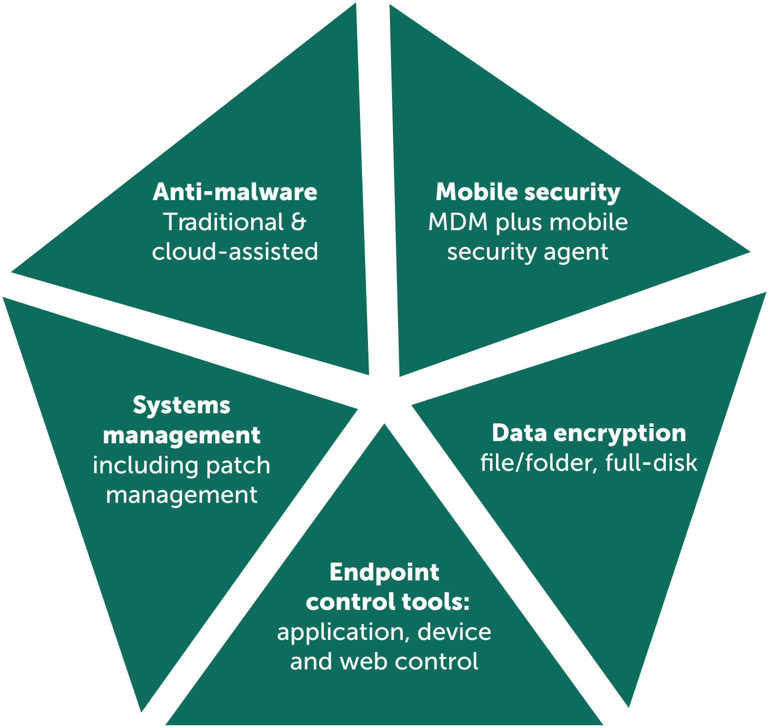
Benefits of Kaspersky Lab's Anti-Phishing Technologies

- Comprehensive approach: the same link undergoes up to three different checks before being classified as secure;
- Minimal response time: Kaspersky Lab's anti-phishing technologies protect users from even the most recent phishing campaigns;
- Proactive protection: Kaspersky Lab's heuristic anti-phishing module can identify a phishing web page even if it is not yet added to the database;
- Early warning: The Kaspersky URL Advisor reputation service identifies phishing links in the browser without having to follow any dubious links.

The protection that Kaspersky Endpoint Security for Business (KESB) offers with its advanced anti-phishing technologies amounts to more than a mere set of mechanisms for handling specific threats. This is an integrated solution that makes the online experience of users secure, no matter how sophisticated the fraudulent schemes devised by cybercriminals might be.

Kaspersky security for business

PHYSICAL » VIRTUAL » MOBILE »



Anti-malware
Traditional &
cloud-assisted

Mobile security
MDM plus mobile
security agent

Systems management
including patch
management

Data encryption
file/folder, full-disk

Endpoint control tools:
application, device
and web control

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

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.

www.kaspersky.com/business