KASPERSKY lab

THE EVOLUTION OF PHISHING ATTACKS:

2011-2013

Overview

June 2013

Just a few years ago, phishing attacks were primarily seen by researchers as just one of several threats found in email spam. For some time, phishing remained relatively primitive from a technical point of view. It was relatively rare and it typically posed a threat only to the most naïve and inexperienced users. But today, the scale of these attacks and the technologies used are such that phishing has been elevated to a category of its own, meriting a separate study.

Phishing is a kind of malicious attack where cybercriminals create a fake website — 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.

If a cybercriminal's goal is to get his hands on a victim's money, then the fake website may contain a field for users to enter their first and last names, contact data, and credit card information.

Sometimes a malicious user may want to collect as much information as possible from his victims, and in this case, the fake website may contain an entire form with dozens of data entry fields.

Although the specific targets of phishing attacks vary, the end goal of all malicious users engaged in this type of malicious activity is ultimately the same: to make money illegally.

This goal is achieved either by directly stealing cash from the victim, as in the case with fake online banking service pages, online storefronts, and subscriptions to online games. However, malicious users may also employ a more indirect approach, i.e., the sale of stolen databases on the black market. A large collection of user data may come in handy for malicious users for a number of different fraudulent schemes involving spam mailings and the spread of malware.

For the purposes of this study, we analyzed data from the Kaspersky Security Network cloud service on all threats encountered on computers running Kaspersky Lab products. Data on KSN is transferred anonymously. Users who consent to participate in this service contribute to higher security levels, particularly for their own computer, but for other participating users as well. The more data available about threats on KSN, the more often it is updated, and the greater the number of threats against which Kaspersky Lab product users are protected. Over 60 million users around the world participate in the Kaspersky Security Network.

By examining KSN data, we were able to conduct a study to establish just how widespread phishing is, where most phishing victims and sources are located, and a list of the main types of websites and online services that are used most frequently by cybercriminals to defraud Internet users.

Methodology

Data Sources:

- Users with Kaspersky Lab products who have consented to anonymously contribute their data on detected threats to the Kaspersky Security Network cloud;
- Data obtained from 50 million individual users;
- Computers running Windows;
- Studies conducted by Kaspersky Lab experts.

Reporting period: For the purposes of this report, data from 2011-2013 was analyzed (two equal periods, each extending from May 1 in one year through to April 30 of the following year).

During the study, the following parameters were analyzed:

- The total volume of registered phishing attacks over a specific period;
- The channels via which links to phishing webpages are delivered;
- The geography and number of attack victims;
- The geography and number of attack sources;
- The classification of attack targets (websites most frequently copied by malicious users);
- Changes in attack targets depending on the targeted country.

Important note: during this study, Kaspersky Lab identified a large number of attacks against banks all over the world. The names of these banks have been deliberately redacted from the text of the study in order to avoid harming the reputations of these banks.

Main Findings

- In 2012-2013, 37.3 million users around the world were subjected to phishing attacks — up 87% from 2011-2012
- Most often, phishing attacks targeted users in Russia, the US, India, Vietnam and the UK
- Phishing attacks were most frequently launched from the US, the UK, Germany, Russia and India
- Yahoo!, Google, Facebook and Amazon are top targets of malicious users. Online game services, online payment systems, and the websites of banks and other credit and financial organizations are also common targets
- Over 20% of all attacks targeted banks and other credit and financial organizations
- The number of distinct sources of attacks in 2012 and 2013 increased 3.3 times
- More than one-half (56.1%) of all identified sources of phishing attacks were located in just 10 countries
- In 2012-2013, 102,100 Internet users around the world were subjected to phishing attacks every day. This is double the amount of intended victims over the previous period
- More than 50% of the total number of individual targets (921 names out of 1,739 in the KSN database) were fake copies of the websites of banks and other credit and financial organizations
- Phishing has some local accents: phisher targets are different from country to country, depending on the popularity of local online resources

Part I:
How do they get your money and personal data?

Phishing scenarios: how do they make you play their game

Before we get to the results of the study, it is helpful to describe the situations in which a user may encounter phishing, and which technologies are used by phishers.

There are numerous examples of fraudulent schemes involving phishing.

In particular, phishing is often used by cybercriminals engaged in text message scams, where users are tricked into visiting a falsified page of a social network and then, under various pretexts, are encouraged to subscribe to a paid text message service. This type of malicious activity is often used in scams where the malicious user tricks victims into giving him their money by pretending to work for a tax or law enforcement agency. With these schemes, victims will receive an email notifying them of unpaid taxes or fines, with a link to a website that allegedly will provide them more information or conduct a transfer of the stated funds to the malicious users.

Phishing is also used in schemes involving fake antivirus products: malicious users make fake versions of websites of well-known security solution developers, in addition to interfaces of well-known antivirus programs to scare users with messages about the alleged detection of threats on their computers, and extorting money for protection against these threats.

Furthermore, phishing may be used as one step in a targeted attack against one or several organizations. One example is when all a malicious user has to do is make a fake web interface to access the corporate email system of an organization, and then lure staff members to the fake site. As a result, the criminal will gain access to confidential correspondence at the very least. In the worst case scenario, the email account data will match up with authorization data for employee workstations and the malicious user will then have the information needed to remotely connect to that employee's work computer.

Ways of deception: from fake websites to malware & XXS vulnerabilities

Phishers use several different methods to trick their potential victims. In addition to the obvious need to create a detailed copy of a website that will be used to attack the victim, the criminals also prepare their cover story by using similar website URLs, replacing one or several characters in the name of the website, or using recognizable website names in the sub-domains. If the delivery channel for a phishing link is email or electronic documents (.doc, .odf, or others), malicious users will often resort to the hyperlink features typically available in most text editors and email clients. In this case, the text of the email or document will display the link to the real site, but the link will actually lead to the website created by the malicious users.

Incidentally, for cautious, experienced Internet users who pay attention to the contents of address strings and check to see if the link and the embedded URL match up, these attacks may not pose much of a threat. However, the cybercriminals frequently use more sophisticated methods of trickery that may not be immediately obvious to the untrained eye.

In particular, by using JavaScript, which is built into most modern browsers, malicious users can try to trick users by displaying the URL of the actual website address in a window with the open phishing website. This is actually put together using JavaScript to display the URL, and users will only be able to see that this is a trick by disabling JavaScript in the browser settings.

Phishing schemes that use XSS (Cross Site Scripting) pose an even greater threat to a user network — in this case even cautious and well-informed users are at risk. With this scam, cybercriminals use a vulnerability in a real website being accessed by the user. By using this vulnerability in the website's server, the phisher can seed random code into the HTTP page generated on the website's server. This code may display a bogus window to enter authorization data. In practice, this allows malicious users to stealthily steal any data that the user enters when interacting with a website.

There is another especially dangerous type of phishing that uses a modification of the Hosts file on victim computers.

In this case, the user's computer is infected with a special malicious program (such as the QHost family, for example), which changes the Hosts file and replaces it with letter-based URL addresses to actual websites via which the attacks are planned, and the IP addresses of the malicious users' servers where the fake versions of these sites have been developed. The way in which any browser running on Windows works is such that any time a user enters an address in the URL field and clicks on "go", the browser first checks the contents of the Hosts file. If the address entered by the user is contained in the Hosts file and is associated with the server's IP address, then the browser will use that same IP address to make the connection. This function is built into Windows by default, including for the establishment of connections to a company's internal electronic resources that cannot be accessed from outside. What's more, theoretically the use of entries in the Hosts files will speed up the connection process with websites, since once it finds the data it needs for the connection in the Hosts file, the browser will not try to contact remote DNS servers for data about which alpha address matches the IP address. Malicious users take advantage of this and use malware like QHost to point to a website's actual alpha address and match it up with the IP address of their own server, which hosts the fake copy of the online resource's web page. As a result, even an experienced user will not notice the switch.

Malicious programs that change DNS server addresses (such as the DNSChanger, for example) used by the computer to route requests sent via the browser work in a similar way, but in a slightly different subsystem of the machine. By default, settings already include the DNS server addresses for network connections recommended by the computer owner's Internet service provider. Trojans like DNSChanger switch these addresses for DNS server addresses owned by malicious users, and as a result, criminals gain the ability to redirect users to any website, regardless of whether or not that address was actually entered in the browser.

Just as with XSS phishing, this type of threat cannot be countered without using security solutions capable of recognizing an attack.

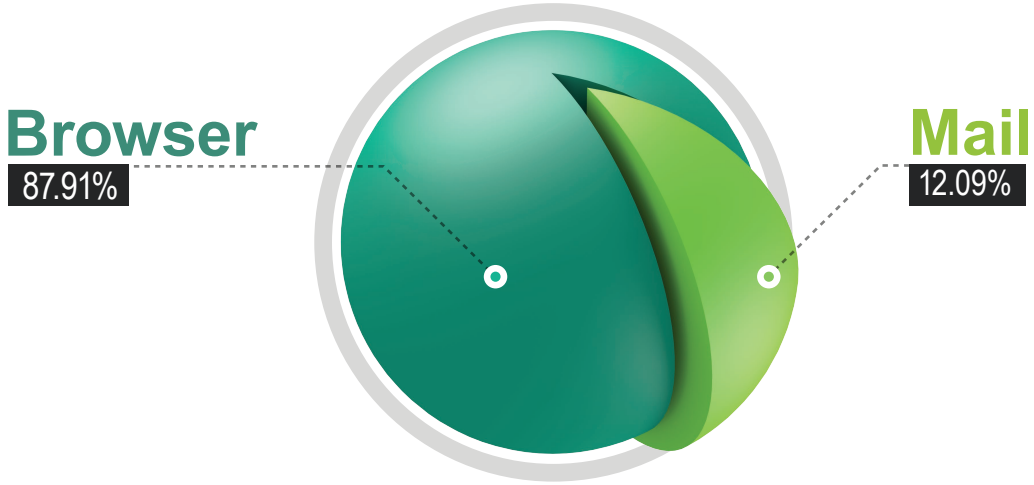
At the same time, the nature of phishing attacks is such that the simplest types can be launched without any major infrastructure investments or in-depth technological research. This situation has led to its own form of “commercialization” of these types of attacks, and phishing is now being almost industrialized, both by cybercriminals with professional technological skills and IT dilettantes.

Overall, the effectiveness of phishing, combined with its profitability for criminals and the simplicity of the process, has led to a steadily rising number of these types of incidents.

Part II:
The increasing threat

There are two ways in which Internet users might encounter links to phishing sites: one is by surfing the web, and the other is by working with email. During this study, we were able to determine that the overwhelming majority of phishing attacks are launched against users when they are surfing the web.

The top 2 ways in which phishing links are spread



It's easiest to encounter a link on a phishing site while using the Internet: banners to legitimate websites, messages on forums and blogs, and private messages on social networks can all turn out to be a ruse.

Although phishing links are encountered much less frequently in email than on the Internet, over the course of one year, phishing schemes in email still rose 1.86 percentage points from 10.23% in 2011 - 2012 up to 12.09% in 2012 - 2013.

A percentage point is a unit used to compare amounts expressed in percentages over various periods of time. For example, if the volume of phishing in email over the course of one year amounted to 10.23%, and 12.09% the next, then over that year, the percentage rose by 2 percentage points (although in typical percentage terms, the amount of growth would be equal to approximately 17%). In this study, when comparing two amounts expressed in percentages, changes will be stated in percentage points.

By using these two channels as vehicles for phishing links, phishers attacked 37.3 million Internet users around the world in 2012-2013, up from 19.9 million in the previous year.

The worldwide dynamics of phishing attacks

Over the year, the number of users attacked around the world rose by approximately 87%, or roughly 17.4 million Internet users in absolute terms.

Most of the victims in 2012-2013 were Internet users living in Russia, the US, India, Germany, Vietnam, the UK, France, Italy, China and Ukraine. These 10 countries were home to 64.05% of all phishing attack victims within the stated period.

In addition to a rise in the number of users attacked, the number of servers involved in phishing attacks also increased.

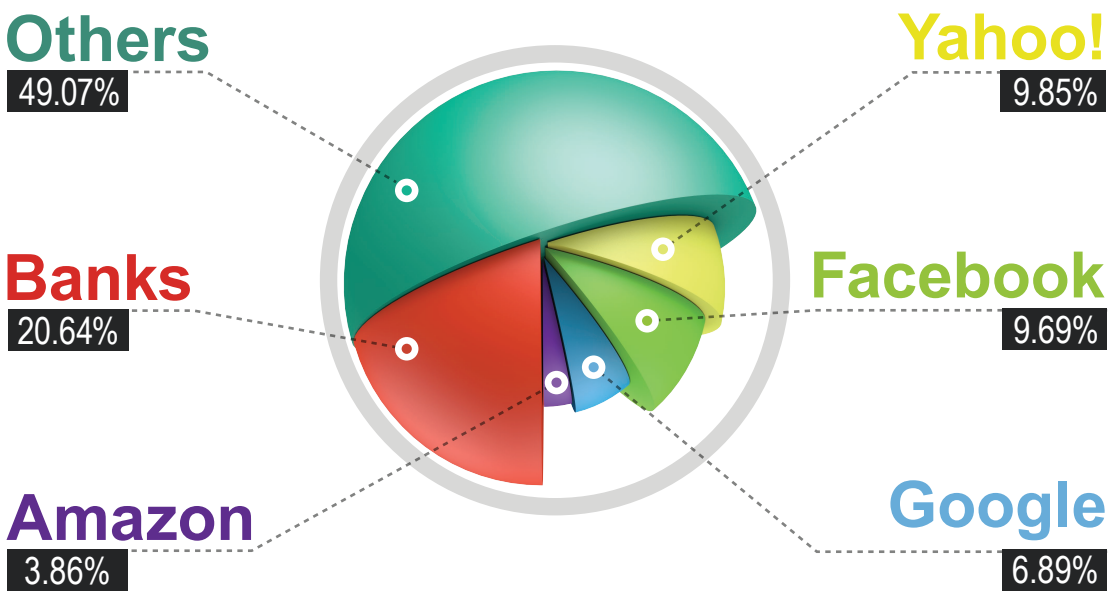
The number of distinct sources of the attack

The number of distinct sources of phishing attacks in 2012-2013 rose 3.3 times. Most of the servers hosting phishing websites were located in the US, the UK, Germany, Russia, India, Canada, France, Australia, Ukraine, and Italy.

The number of phishing attacks against users nearly doubled, while the number of sources of attacks tripled.

More often than not, these servers hosted fake copies of search engine websites like Yahoo! and Google, in addition to Facebook and Amazon.

Most targeted: Social, Search, Banks



Total number of identified targets: 1,739

In total, 30.29% of all identified phishing links led to webpages mentioning Yahoo!, Facebook, Google, and Amazon. The next most common targets included banks and other financial organizations, representing 20.64% of all identified attacks.

The list of most frequent targets includes search engines and email services, social networks, online stores and auction venues, online gaming services, blogs, banks, and other types of credit and financial organizations, as well as payment systems, IT company websites, and telecom operator websites. In a nutshell, these are all major Internet resources where malicious users might have a chance of extracting some valuable personal data from users.

This is the general picture of the development of phishing threats on a global level. The number of users that are being attacked has nearly doubled, while the number of sources of attacks has tripled.

Meanwhile, the data obtained from Kaspersky Security Network can help conduct a more in-depth analysis of the developments over the past two years.

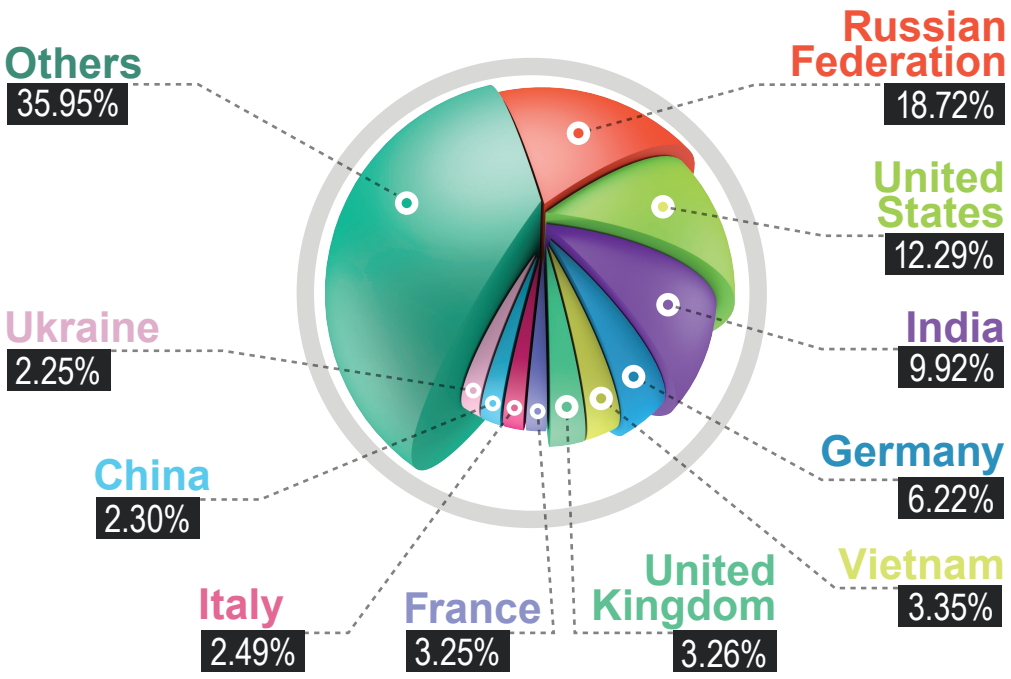
Part III:
Geography of Phishing

TOP 10 attacked countries

The Top 10 countries most frequently targeted by phishers did not really change in 2012-2013 from 2011-2012. The only changes that took place involved the percentage of targeted users in those countries where phishing attacks were registered.

For example, Russia is still in first place in terms of the number of users attacked, even though its share of attacks fell by 3.74 percentage points. China's percentage also saw a significant decline: in 2011 - 2012, the percentage of users in China subjected to phishing attacks was 3.85% of the total number of phishing victims over that period, which put it in fifth place among the most frequently targeted countries. However, at the close of the following period, Chinese users accounted for just 2.30% of all attack victims, which put China in ninth place in the ratings. Other countries with slight decreases in the volume of attacks were the UK, France, and Ukraine.

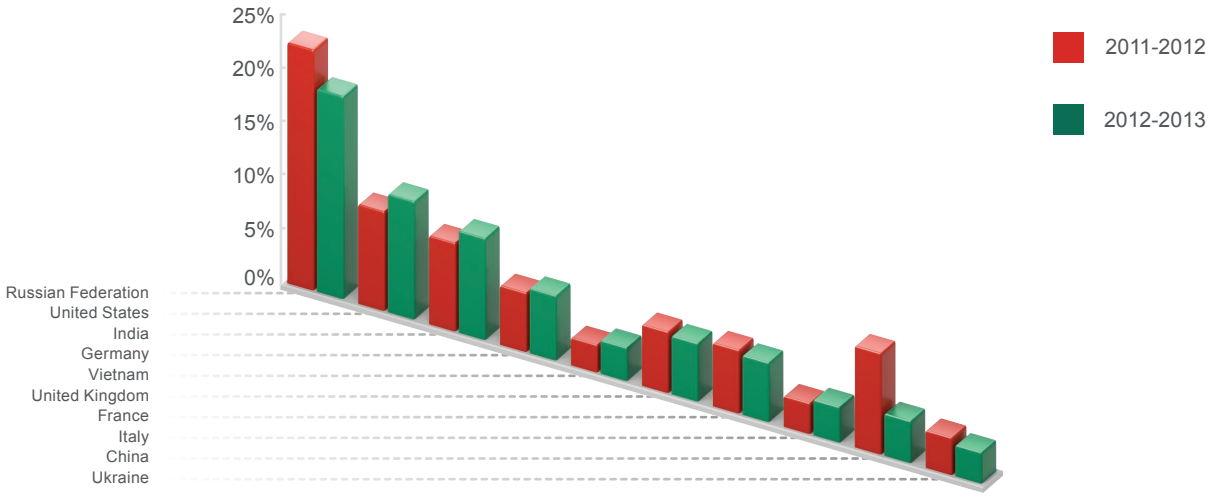
Top 10 attacked countries in 2012-2013



Data from 240 countries over 2012-2013

The percentage of attacks against users in the US rose from 9.83% in 2011-2012 to 12.29% in 2012-2013. The percentage of users attacked in India, Germany, and Vietnam also rose, but at slower rates.

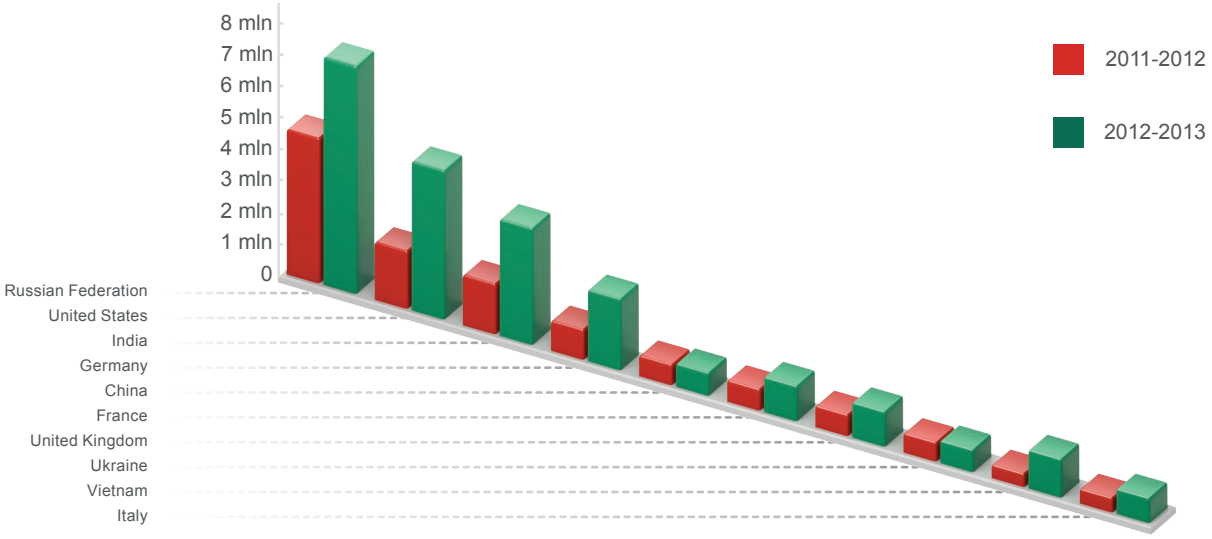
Top 10 attacked countries in 2011-2013



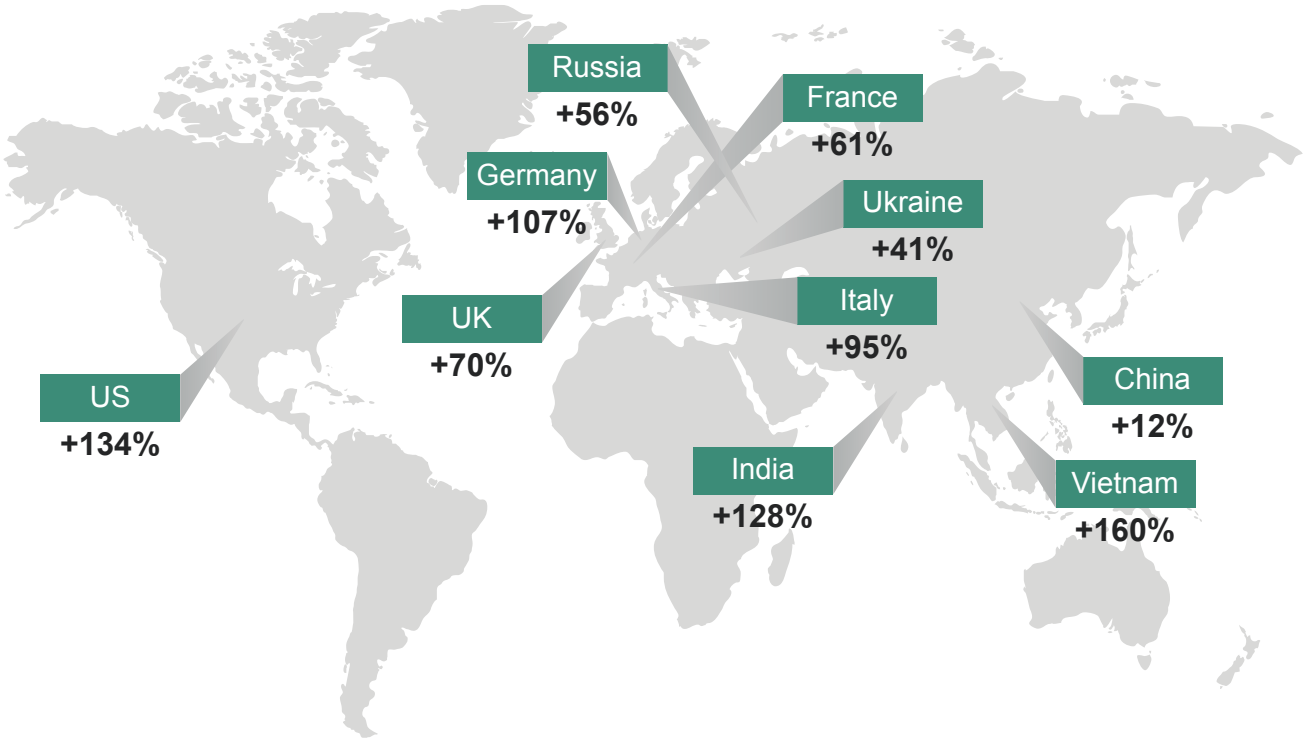
Although the percentage of phishing targets in many countries did decrease, the number of attacks in various countries is still on the rise. For example, the number of users attacked in Russia over the last year rose by 56.1% from 4.47 to 6.98 million users. And while Russia is in first place in terms of the number of victims, its 50% growth is still not the largest growth rate in this category. The number of users subjected to phishing attacks in Vietnam increased over 2.5 times over the past year from 480,000 up to 1.2 million.

In 2012-2013, 102,100 users around the world were subjected to phishing attacks. That is double the number of victims in 2011 - 2012.

In the US, the number of users targeted in phishing attacks rose 2.3 times from 1.9 million up to 4.5 million. This indicator was 2.2 times in India, where the number of phishing victims rose from 1.62 million to 3.7 million. The number of Internet users subjected to phishing attacks doubled in both Germany (2.3 million in 2012-2013) and Italy (930,000 in 2012-2013).



There was comparatively low growth in the number of attacks registered in China, where “just” 858,000 users were subjected to phishing attacks in 2012-2013, against 767,000 in 2011-2012. The Top 10 countries with the highest growth rate in phishing attacks are



Based on the absolute number of users attacked over the year, it’s not difficult to calculate just how many users were subjected to attacks daily.

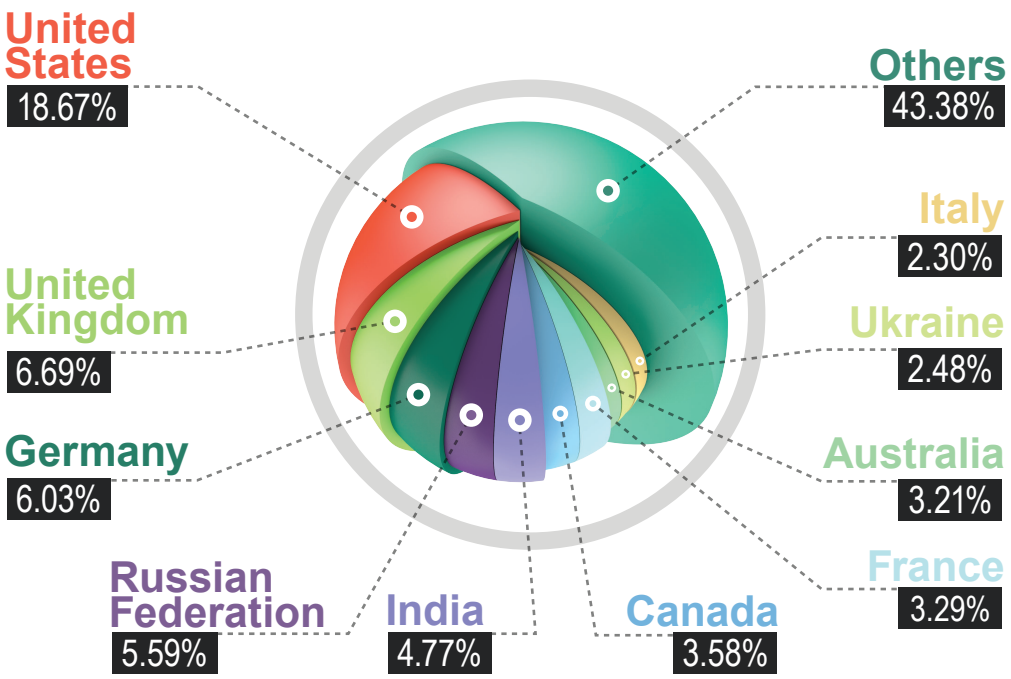
In 2012-2013, 102,100 users around the world were subjected to phishing attacks on a daily basis. In Russia, 19,000 users were attacked each day, 12,000 in the US, 10,000 in India, 6,000 in Germany, 3,000 in France, and another 3,000 in the UK. During the previous year these numbers were much lower. Over the period from May 1, 2011, through April 30 2012, nearly 52,000 users around the world were subjected to phishing attacks daily. On average, 12,000 users were attacked in Russia, 5,000 in the US, 4,000 in India, 3,000 in Germany, 2,000 in France, and 1,000 users in the UK.

Overall, the volume and intensity of phishing attacks has more than doubled over the past two years. Even so, the ‘big picture’ of the evolution of phishing threats wouldn’t be complete without an analysis of the locations of the sources of these attacks.

Where are phishing attacks coming from?

The Top 10 countries where most malicious servers are located are very different from the Top 10 targeted countries.

The location of hostile servers in 2012-2013



As the chart above illustrates, the US was the number one source of phishing attacks in 2012-2013. The US is not only in a leading position when it comes to the number of hostile phishing hosts, but compared to 2011-2012, it also saw a 5.89 percentage point growth in the overall volume of all identified attack sources. No other country saw such large increases in its overall volume of phishing sources.

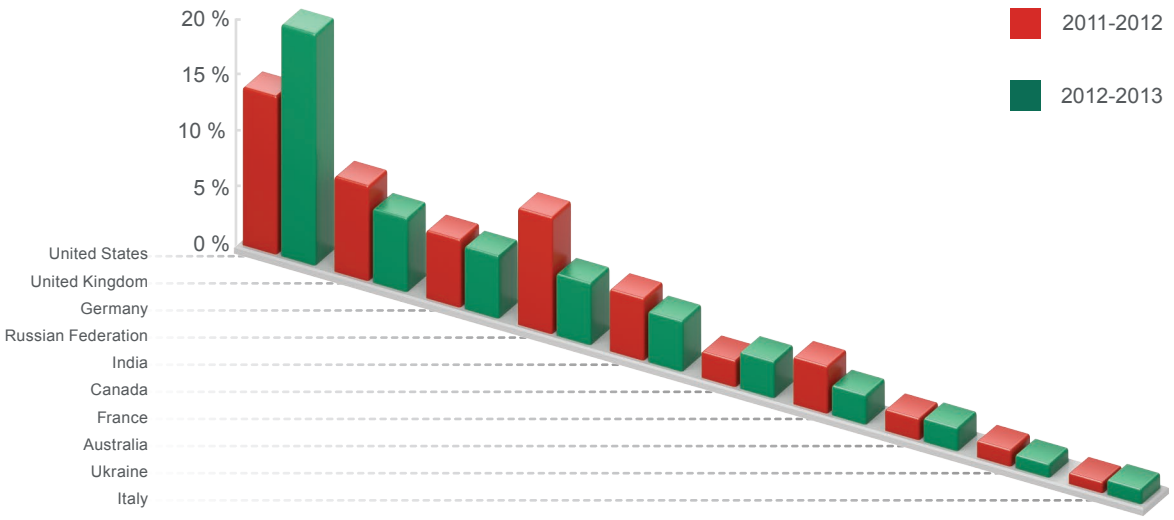
Together, the Top 10 phishing sources account for 56.61% of all identified sources of phishing attacks.

There are also countries in the Top 10 that have experienced a substantial decrease when it comes to their so-called 'contribution' to the total number of phishing link sources. Russia turned out to have the largest decline, as its share fell from 9.55% to 5.59%. The number of attack sources in India also fell by 0.92 percentage points down to 4.77%, and 0.89 percentage points down to 3.29% in France. UK-based phishing sources also fell by 0.88 percentage points, coming in at 6.69%.

Compared to the Top 10 countries targeted in phishing attacks, the Top 10 sources of phishing have two newcomers: Canada and Australia, which took 6th and 8th place, respectively. Canada accounted for 3.58% of sources, and Australia for 3.21%. These countries both saw an increase in the number of phishing attack sources from the previous period: Canada gained 0.31 percentage points, while Australia's share rose by 1.14 percentage points.

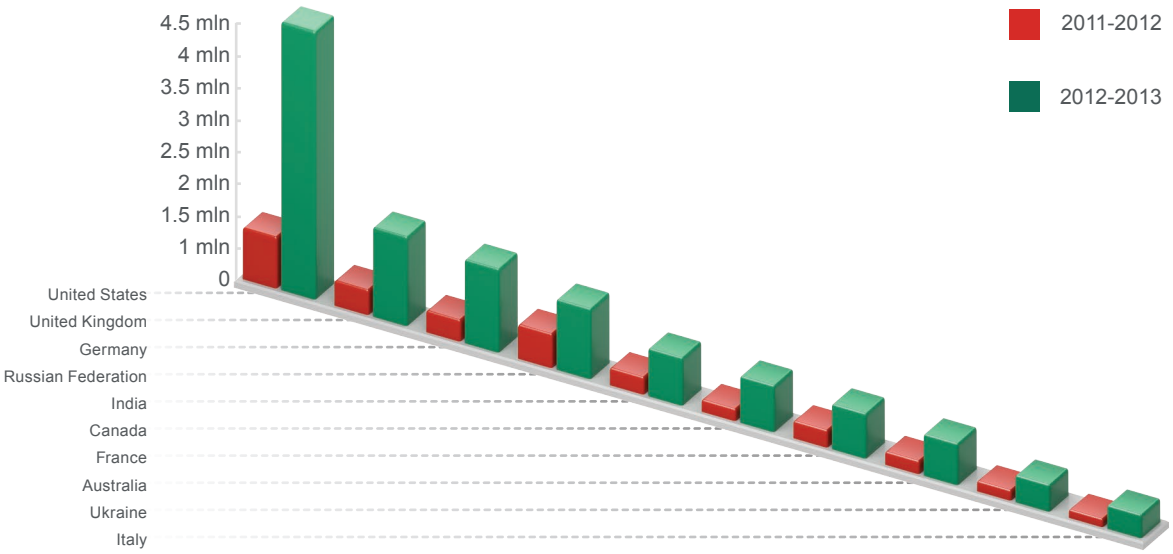
The US is not only the top country in terms of the number of hostile phishing hosts (18.67% of all phishing attack sources), but also demonstrated the most growth since 2011-2012, with a rise of 5.89 percentage points in the number of identifiable sources of phishing attacks.

The location of hostile servers in 2011-2013

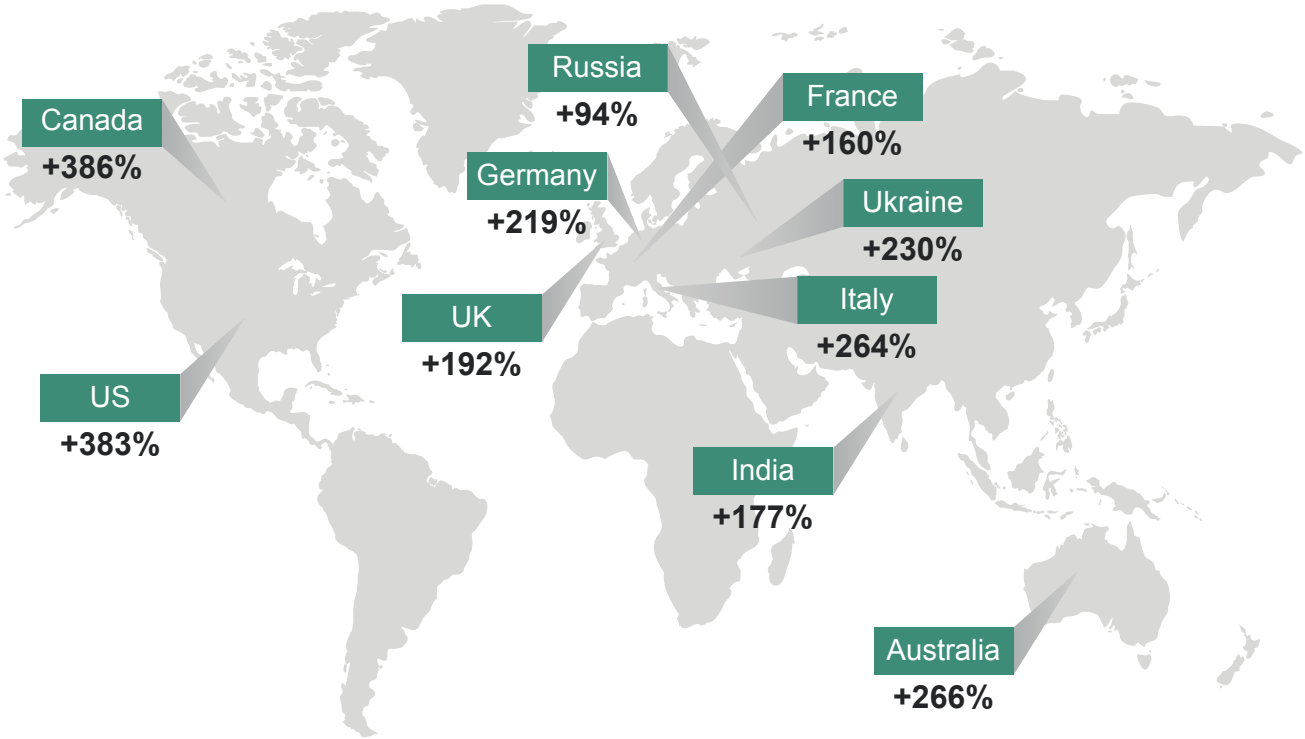


Again, just as we saw with the number of attacked users, a decrease in the percentages of some countries in the total volume of identifiable sources of phishing attacks does not imply an actual decrease in the number of actual sources. This indicator, by contrast, increased in all countries.

The number of distinct hosts in 2011-2013



The Top 10 countries hosting the most phishing attacks and with increased numbers of identifiable attack sources:



KASPERSKY lab

Canada, the US and Australia have a firm lead in this category, noticeably ahead of the others in the Top 10. The slowest growth was noted in India, France, and Russia.

There are several possible reasons for the changes in the Top 10 sources of phishing attacks over the past year; changes may have been provoked by regulatory and policy changes affecting the Internet and making phishing more of a risk in terms of liability, thus involving more time and effort to develop a working infrastructure. An increase in the number of available hosting services offering high levels of client anonymity and other factors may have also played a part. But no matter the reasons, the numbers show that over the past year, the list of countries hosting the largest numbers of phishing web pages has not changed. Together, the Top 10 represents approximately 56.61% of all identifiable sources of phishing attacks.

Information about the number and geography of phishing attack victims and sources help us to understand the scale of the threat posed by phishing, although the question of just how the cybercriminals obtain the valuable data they are after in their attempts to draw users' attention and trick their potential victims remains unanswered. But we have gained some insight from analyzing data about the websites that phishers most often copy.

Part IV:
Top phishing attack targets

Over the last year, Kaspersky Security Network has identified 1,739 unique targets (companies and services whose sites were copied by phishers), which is 250 more than in the previous year. This time, as expected, targets included social networks, search engines and email services, telecom companies, e-payment services, banks, and other credit and financial institutions. However, there were a few surprises as well, such as tax and customs agencies, the governments of various countries, car companies, insurance companies, medical institutions, oil companies, and transportation companies (including some airlines).

Criminals target not only typical users but also their own kind. In 2012-2013, Kaspersky Security Network registered over 9,000 distinct attacks (nearly five times more than in the prior year) against Liberty Reserve. The electronic currency of this service is actively used by cybercriminals around the world in order to pay for various illegitimate services and conduct financial machinations.

Furthermore, malicious users have also copied the websites of media outlets, reference and information services in finance and security, as well as online storefronts used to sell shoes, clothing, electronics, furniture — and in one case, a country music television channel.

The abundance of different industries and subject matters among the targets just goes to show that phishers will use any and every opportunity to get their hands on other peoples' personal data and money — even if it means the data and money is from other players in the Internet underworld. For example, in 2012-2013, Kaspersky Security Network registered over 9,000 unique attacks (nearly five times more than in the previous year) against Liberty Reserve. This service offered an electronic currency until it was shut down by the US authorities this spring. For years that currency had been extensively used by cybercriminals around the world to pay for various illegitimate services and conduct financial machinations.

Incidentally, the variety in the type of targets says nothing about the most common preferences among cybercriminals when selecting their targets.

Along these lines, another figure holds more meaning: over 50% of the total number of individual targets (921 of the 1,739 listed in the Kaspersky Security Network database) were fake copies of the websites of banks and other credit and financial organizations around the world. That figure does not include e-payment systems such as Visa or MasterCard, as well as other types of e-money.

Within that subcategory, the lion's share (at least 70%) of distinct targets are bank websites, and in the other cases the targets involve fake copies of websites for a variety of investment funds, credit unions, and other organizations engaged in financial operations. Compared with the previous period (2011-2012), there were no real changes, as over half of the total number of unique targets were banks.

All the same, this large number of individual targets in finance does not mean that one-half of all phishing attacks target banks. Although the names of various banks are mentioned in KSN statistics, the majority of these attacks were of a very small scale, with less than 10 unique incidents per year.

At the same time, it makes sense to consider an attack a threat if it affects a large number of users. From that viewpoint, the percentage of attacks launched against banks and credit and financial organizations is considerably lower than 50%, although large nonetheless. Approximately 20.64% of all distinct attacks registered during 2012-2013 were launched against these types of targets. Only well-known sites such as Yahoo!, Facebook, Google and Amazon are targeted more frequently (30.29% of all attacks), so there are other "leaders."

The number of users = the value of target

The more popular a website is, the more frequently malicious users copy it and, as a result, there is a higher probability that a user will run into a fake version as he surfs the web.

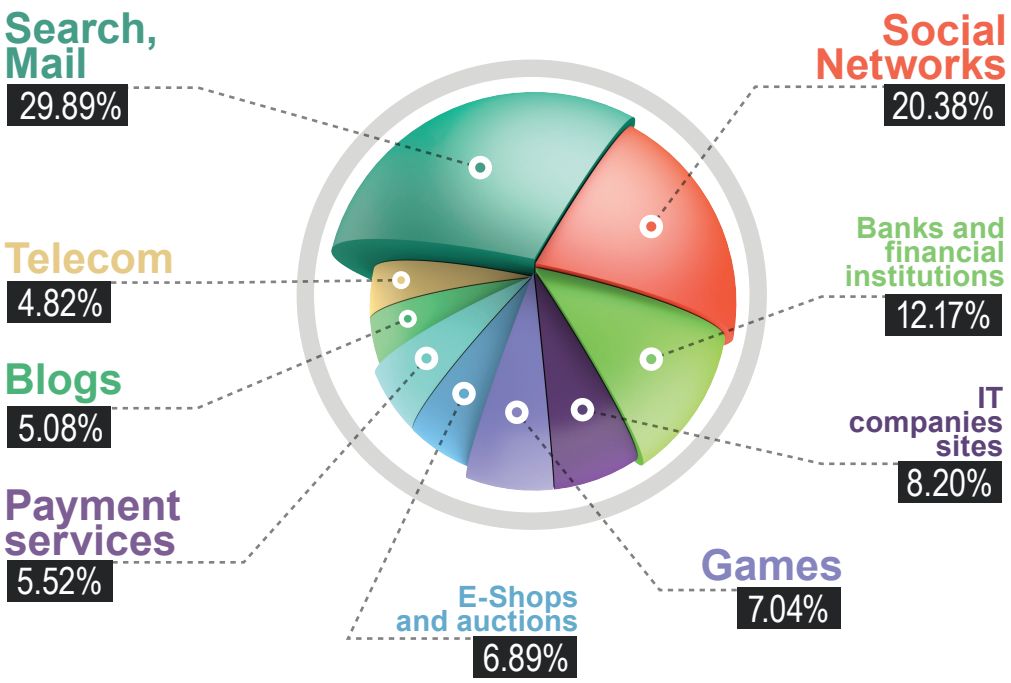
Over 50% of the total number of distinct targets (921 of the 1,739 in the Kaspersky Security Network database) are fake copies of the websites of banks and other credit and financial institutions around the world.

In order to build an overview of the situation that is as realistic as possible, the types of targets that pose the greatest threats were ranked, and we compiled the Top 30 targeted websites and grouped them by type. The Top 30 targets account for 65% of all distinct attacks registered over the course of the year.

The selected method helps to more precisely determine the type of targets that were encountered most often by users over the reporting period. Our ranking of the most common types of targets from the total list of attacks would not have produced any relevant results since, as the example with bank phishing has shown, a large number of distinct targets does not necessarily mean that a large number of attacks were launched. However, a large number of distinct targets against which a small number of attacks were launched over the course of the year does produce a significant figure, but it does not convey just how intense the attacks were and does not illustrate the actual scale of a threat, unlike the rankings calculated for the Top 30.

As a result of this analysis, the websites that were most often copied fall into nine different types of online resources:

Types of targets in 2012-2013



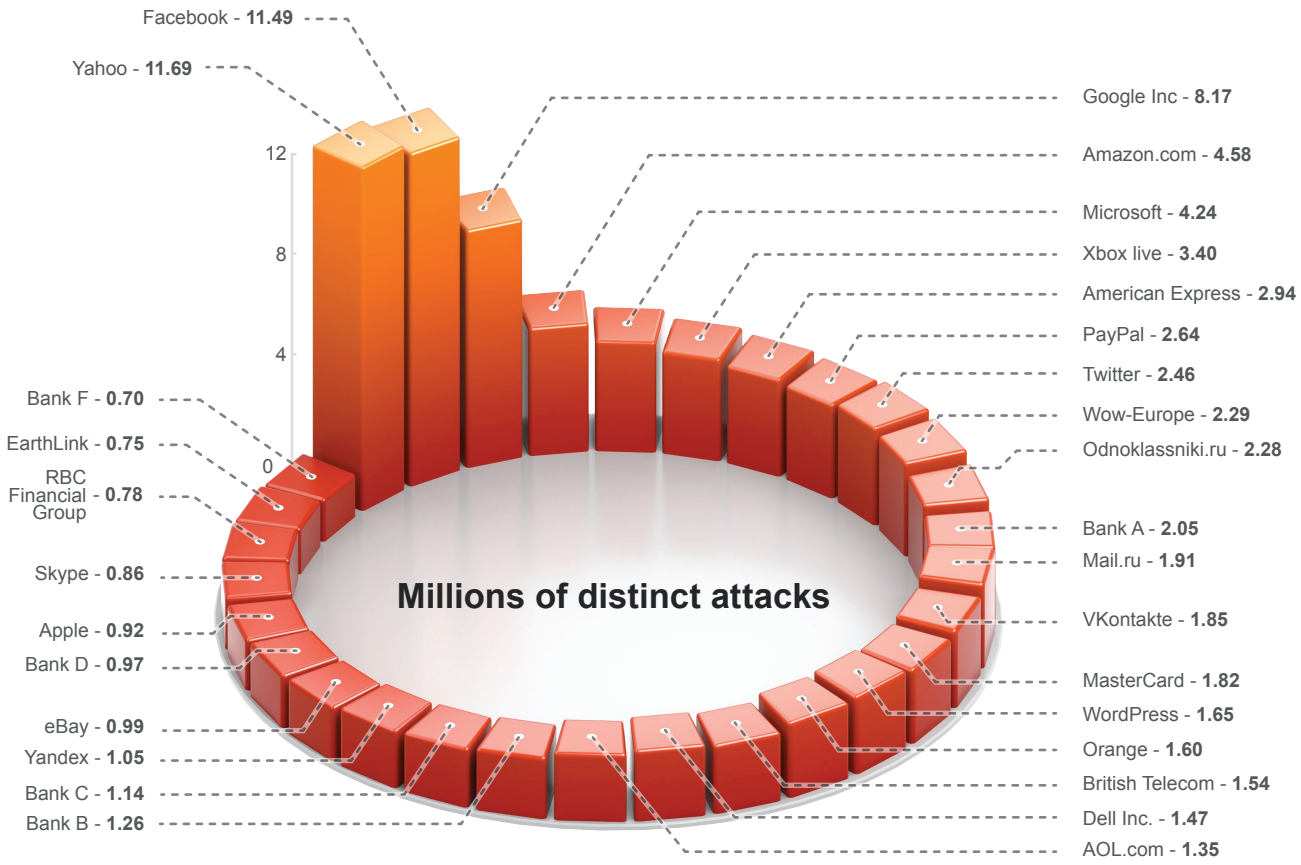
Compared to the numbers from 2011-2012, over the past year the types of sites in this rating that are most often copied by malicious users underwent some substantial changes. In particular, the percentage of search engines and email services fell by 10.53 percentage points from 40.42% to 29.89%. In addition to email and search services, a considerable decrease was seen in the amount of e-payment services, which fell from 7.83% to 5.52% in 2012-2013.

In contrast, the percentage of social networks rose slightly from 18.16% up to 20.38%. The percentage of fake online stores and auction venues more than doubled, accounting for 6.89% of all phishing attacks in 2012-2013, against 3.60% in 2011-2012. The number of fake websites copying banks and other financial organizations also rose considerably, from 9.78% of such attacks in the Top 30 in 2011-2012 to 12.17% in 2012-2013.

These numbers demonstrate that cybercriminals are more frequently resorting to phishing in an attempt to steal money or valuable financial information directly from users. At the very least, the growth rate of attacks against online storefronts and banks speaks to the increased interest among malicious users in these types of websites.

The chart below shows the most frequently attacked websites, without breaking down the Top 30 by type.

Top 30 targets in 2012-2013



Over the past year, the Top 30 most copied sites did not undergo any major changes. Just like in the prior ratings, the only changes that were recorded were the percentages of targeted websites in the total number of attacks.

For example, the percentage of attacks involving pages copying Yahoo! services fell from 15.29% in 2011-2012 to 9.85% in 2012-2013, which nonetheless did not push Yahoo! out of its position of most targeted website. A considerable drop was seen in Google's percentage as well, from 9.17% to 6.89% of all attacks. At the same time, attacks involving fake Facebook pages rose, accounting for 9.69% in 2012-2013. This rise pushed Facebook up from third to second place in the ratings.

There were substantial changes in the percentage of attacks involving fake websites purporting to be Amazon.com. In May 1, 2011 through April 30 2012, the percentage of attacks involving a phony Amazon site came to 1.44% — compare that to 3.57% in 2012-2013. Over one year, Amazon climbed from 15th to 4th place in the ratings.

The growth rate among attacks targeting online stores and banks highlights the increased interest of malicious users in these types of sites.

Malicious users have also started making phony websites designed to look like MasterCard system services, in addition a prominent bank (Bank A), the Russian VKontakte social network, and Twitter — their percentages all changed only slightly, but all changes were increases.

The Top 30 websites that are copied the most often by phishers are mostly services and companies whose names are known by a mass audience. The number of attacks against one or another online resource may correspond directly to its popularity. For example, the percentage of attacks involving phony Yahoo! sites in the total phishing volumes has fallen alongside the company's decreased share of the web search market and other online services, while Amazon's percentage has grown markedly, in line with the company's success on the e-commerce market and the successful launch of its tablets. Incidentally, we know that the connection between a company's standing on the market and fluctuations in phishing attacks involving copies of that company's websites are relative. Although a general connection between a website's popularity and the number of phishing attacks launched against it certainly exists, unknown online resources are typically left alone by phishers.

National traits

In order to boost the effectiveness of phishing attacks, cybercriminals strive to set up and launch them to ensure that there are as many potential victims as possible. However, depending on the country, the list of the websites that are visited may change — this is typically influenced by local user preferences. Kaspersky Lab's study provides evidence that malicious users factor in these aspects and as a result the most frequently copied websites vary from country to country.

Neither the Russian nor Ukrainian Top 10 most copied websites feature even one financial organization, while local ratings in other, more frequently attacked countries feature several financial organizations.

For example, a local threat rating typical for the US in 2012-2013 matched up with the global Top 10 only for the first four rankings: Yahoo!, Facebook, Google, and Amazon are used most often in phishing attacks targeting US-based Internet users.

However, further down the list, we see some big differences. In particular, more than anywhere else in the world, US citizens are targeted by phishing schemes involving fake versions of World of Warcraft, Microsoft, AOL, and financial companies like American Express and social networks like Twitter. Compared to the previous reporting period, Amazon experienced some big growth, and climbed from 10th place to 4th.

The same type of situation is still present in other local ratings — the UK Top 10, for example. The top rankings include the same three sites as the US, but there are some substantial differences as you move down the list. In particular, the websites that are most often falsified include the Internet resources of British Telecom, and one of the most prominent British financial conglomerates (Bank E).

Below is a comparative table of the websites that are most targeted by phishers in the US and the UK.

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

If we take a look at the top ratings in other countries, we will see even more country-specific websites.

For example, in France phishing websites using the Yahoo! name are encountered relatively infrequently when compared to the US and UK. In the list of the Top 10 phishing targets in France, Yahoo! ranks sixth. Meanwhile, the national email service La Poste is in third place, right behind Facebook and Google.

In Russia and Ukraine, phishing ratings are vastly different from those of Western countries.

In particular, the first three rankings were the popular social networks Odnoklassniki.ru (for classmates) and VKontakte, as well as the Google Inc search engine. Further, these ratings demonstrate even more country-specific aspects: the Mail.ru email service is in fourth place, and Yandex is in fifth place. Yahoo! and Facebook are also in the Top 10, but they are in sixth and seventh places, respectively. The Ukrainian Top 10 is more or less the same.

Remarkably, neither the Russian nor Ukrainian Top 10 most frequently copied websites feature even one financial organization, while local ratings of the other most frequently attacked countries typically include several financial organizations. Furthermore, these threats are often very representative of national traits.

For example, one of the largest local banks is on India's Top 10 for 2012-2013, right after another bank that operates on a global level. Another large bank (the largest in the country) is in seventh place on Germany's Top 10. Phony websites copying local financial institutions are seen in the Italian, French, and Chinese Top 10s.

Overall, in the Top 10 ratings in eight out of ten different countries where residents were most often subjected to phishing attacks, the attacks were meant to steal either money or valuable financial information. This points to a dangerous general trend.

Conclusions

The information collected from the Kaspersky Security Network cloud service has helped us gain a better understanding of the global landscape of phishing threats from a variety of angles. None of this, however, is particularly optimistic. Both phishing itself and the diversity of the types of phishing attacks are experiencing rapid growth and affecting an enormous number of users and organizations around the world.

It is also important to note that this study addressed only attacks that were intercepted using heuristic security technologies built into Kaspersky Lab products. Naturally, Kaspersky Security Network is unable to provide data about the number of successful phishing attacks, or attacks that are launched against those who are not using Kaspersky Lab security solutions.

The relative simplicity of setting up these types of attacks and the high probability of gaining some type of reward from a successful phishing ploy is attracting more and more malicious users to phishing. Websites and other online services are here to stay, and now part of our daily lives. Checking feeds on social networks, checking email, purchasing goods online, and conducting other financial business via web-based interfaces are all activities that have become commonplace procedures, and it’s easy to overlook some minor design changes in a familiar service or a website’s URL — which is exactly how cybercriminals are able to manipulate Internet users.

Recommendations for consumers

1. Education

An understanding of phishing tactics can help you protect yourself against these types of attacks.

- Even when visiting a site that you are familiar with, don't forget to check for any tell-tale signs to make sure it's the real deal: the address in the URL field should be written without any oddities or mistakes.

- If a friend on a social network or instant messaging service sends you a link, it's worth the extra time to ask what the link goes to. If a link arrives from a friend or someone that you don't know but is from a reputable domain (such as a bank where you hold an account), or if you receive an email with an active hyperlink in the body of the email, take the time to double check it and use the hyperlink editing feature in the text available in just about all email clients these days. If the link in the text says one thing, but the actual link in the editor is something completely different, then you're dealing with a phishing link.

2. Advanced protection technologies

Unfortunately, there are many different phishing methods that cannot be identified without special tools. A computer or mobile device needs to have a quality security solution in place to ensure the safe use of online resources.

- More specifically, a security solution should feature an advanced anti-phishing module. The anti-phishing technology built into Kaspersky Lab products can recognize phishing web pages and follow a set of heuristic rules. In other words, this technology can even identify completely new phishing attacks that have never been seen before.

- The URL Advisor module built into Kaspersky Internet Security and Kaspersky Anti-Virus is another technology that contributes to effective protection against phishing. This module uses a database in the Kaspersky Security Network cloud service to determine the reputation of all of the links on a webpage opened in a user's browser; if any of them are found to be associated with phishing, URL Advisor will immediately notify the user.

- The Safe Money technology available in Kaspersky Internet Security and Kaspersky PURE provides protection against the most dangerous types of phishing schemes, which are specifically designed to steal cash directly from users. It involves a regularly updated database of trusted addresses for online banking systems and e-payment services, and automatically activates whenever a user opens up that type of website. This technology also puts browsers into safe mode to prevent the execution of suspicious code during online banking sessions.

- Kaspersky Mobile Security — Kaspersky Lab's security solution for mobile devices — features anti-phishing technologies and an additional built-in cloud security scan function that, together with Kaspersky Security Network, identifies malicious mobile apps, including fake copies of well-known apps created to steal personal user data.

Recommendations for businesses

1. Education

- The advice above for Internet users to be educated about phishing is appropriate for corporate employees as well, since an employee who knows what phishing is and understands its potential consequences will be more cautious when using the Internet on a company computer.

2. Professional security solution

Phishing can be used as just one of the stages in a targeted attack against your company. The objective of this type of attack could be corporate espionage, or the theft of money from company accounts or the personal accounts of company employees. That is why it is important to use a top-quality security solution for corporate work stations that can provide protection against phishing and spam and offers a wide range of security features, such as Kaspersky Endpoint Security for Business.

- Kaspersky Lab products provide security for all of the different components of a corporate network at all levels, including the gateway and workstation levels. This makes it possible to scan and filter unwanted traffic. What's more, our specialized Kaspersky Security for Mail Server solution effectively counteracts phishing schemes in a company's email traffic.
- The advanced protection against malware offered in Kaspersky Lab products offers a reliable defense against Trojans that change data in the Hosts file and DNS settings.
- Kaspersky Endpoint Security for Business features effective tools to control network access. The Web Control function helps restrict access to specific websites from corporate workstations, greatly reducing the risk of any situations where an employee might fall victim to a phishing scam after visiting a site seeded with malicious content.
- The specialized anti-phishing security solution built into Kaspersky Endpoint Security for Business features an extensive and regularly updated base of phishing web pages, in addition to being able to independently detect phishing pages using a number of heuristic signs. It can also log and block attempts to redirect a user to a phishing page not only from the browser, but, for example, from an online chat service such as Skype
- Special solutions that protect against spam, where phishing emails are often found, are another key element of solid protection against these types of attacks. The anti-spam technology in Kaspersky Lab's corporate solution provides the necessary level of protection against phishing ploys in emails thanks to an extensive and regularly updated signature database of new malicious mailings, as well as phishing email signatures.

- Phishing can be a threat for employees using corporate mobile devices, smartphones, and tablets, which are often used by employees at work in the place of conventional computers or laptops. Kaspersky Lab's Security for Mobile is designed to protect mobile devices and manage them. Among other features, this solution protects against spam and phishing websites, and also has an app control function that prevents the launch of spyware on corporate mobile devices. Kaspersky Security for Mobile is compatible with most of the mobile platforms available today and can help companies quickly and efficiently integrate an employee's personal device into the corporate network.