POSITIVE TECHNOLOGIES

SOCIAL ENGINEERING: HOW THE HUMAN FACTOR PUTS YOUR COMPANY AT RISK

2018

CONTENTS

INTRODUCTION

When cybercriminals want to penetrate the infrastructure of a target company, they increasingly tend to use social engineering to do so. The human factor is still the weakest spot in any protection system, making training on information security awareness for employees more important than ever. An effective way to combat fraud is to simulate attacks in real-world conditions. This tests employees' reactions without any risk of harm to business infrastructure.

Positive Technologies regularly performs assessment of information security awareness among employees at major companies all over the world. This report provides statistics and analysis from 10 most instructive testing projects in 2016 and 2017, including examples of successful attacks against employees. These projects are based on various social engineering techniques and generally included emails, phone conversations, and communication via social networks.

WHITE HATS DRESSED UP IN BLACK

To assess information security awareness among employees, Positive Technologies experts perform a sequence of test attacks, approved in advance by the client, that imitate what real attackers would do. Then the experts track employees' responses. The emails sent by the experts contain a link to a special website, where the employee is asked to enter credentials. These messages may also contain an attachment, which is normally a Microsoft Office document (with executable contents) or archive.

Experts start by collecting employees' email addresses from publicly available sources (just like criminals would do) and provide the results to the client. The client then decides whether to remove or add addresses to the list. Emails are sent only to addresses that are on the domain of the client company. Employees are split into groups, with a separate phishing scenario developed for each group. Applying multiple scenarios allows determining which one works best against a particular client.

After the messages have been sent, the experts collect and analyze statistics. This information shows how many potentially insecure actions the message recipients performed: clicked a link, entered credentials, downloaded and ran a file, or replied to a message. This demonstrates the data that can be obtained by a potential attacker, how an attacker could spread malware on corporate infrastructure, and how an attacker could penetrate the company's intranet.

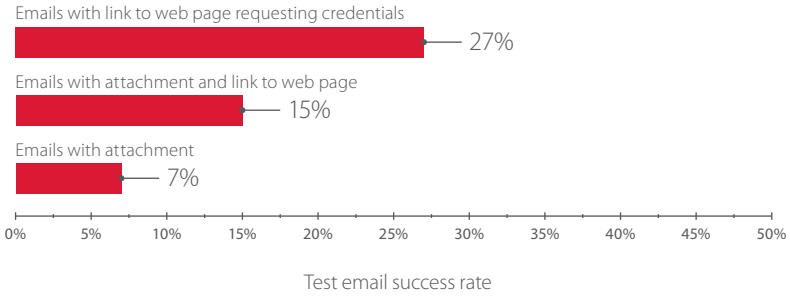
In the 10 projects in question, the experts sent a total of 3,332 emails containing attachments and/or links to websites, some of them with password input forms. The following diagram shows statisctics on the contents of these emails.

Types of test emails

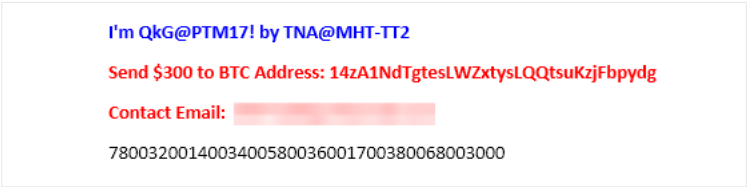
The attached files were harmless, with the experts recording only whether or not the file was run. For cybercriminals, it's often enough that a user simply downloads and opens a file. However, sometimes they need for the user to confirm installation of software or make changes with administrator rights.

17 percent of these emails could have led, in a real attack, to compromise of employees' computers and, consequently, the entire enterprise infrastructure.

As expected, the most successful social engineering technique is the use of a phishing link—27 percent of employees clicked it. Users are not picky when reading the link URL, sometimes clicking it without a second thought. When a user is prompted to download a file and then run it, every additional requested action raises more suspicions. In these cases, only 7 percent of employees were inattentive and fell for the bait.



A real attack scenario could be as follows: An attacker deploys exploits for various software versions on a website. Potential victims receive an email message that links to this website. An employee clicks the link in the email. As soon as the web page loads, vulnerabilities are exploited, which can cause infection of the user's workstation with malware. For example, if the employee opens the link with an obsolete version of browser Internet Explorer, Remote Code Execution (CVE-2016-0189) can be used to obtain total control of the employee's computer. The employee would not even notice that the computer has been hacked. An attachment can contain multiple exploits at the same time, each one aimed at a different software flaw. There is an entire set of vulnerabilities that can be used by an attacker (CVE-2017-0037, CVE-2012-0158, CVE-2017-0199, and others). In November 2017, a group of attackers emailed documents whose payload consisted of ransomware called qkG.[1] If a user downloaded the file and had macros enabled, the ransomware would strike as soon as the file was closed. The contents of all documents on the victim's computer were encrypted and a ransom note was displayed. Meanwhile, the ransomware could continue spreading on corporate infrastructure and start an epidemic.



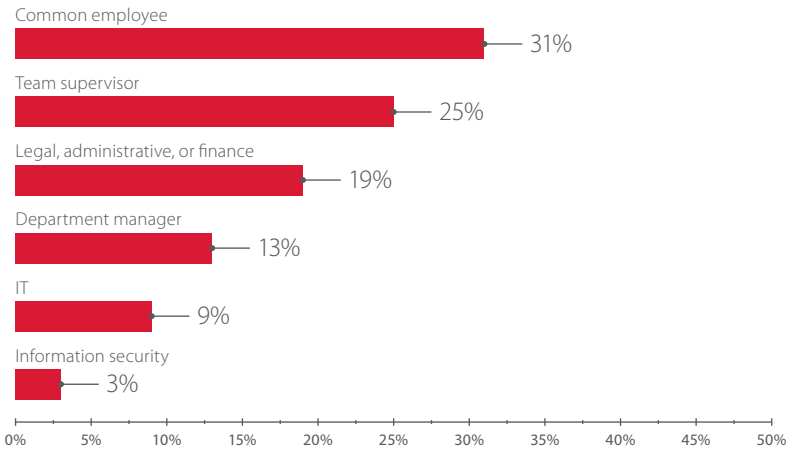
To increase their chances, attackers frequently combine multiple attack techniques. A phishing message might contain an attachment (containing several malicious scripts) and a link to a website (with several exploits and an input field for entering credentials). Even if the target company uses the latest software with all security updates, and even if antivirus software is present and properly configured, this will not prevent situations when a user inadvertently types a password in an entry box on a fake website, putting this information in the hands of criminals.

UNWITTING ACCOMPLICES AT THE WORKPLACE

It should be self-evident why it is a bad idea to click an unknown link, enter credentials on a dubious website, or run a suspicious file. But what is the problem in just talking with an attacker? Let's consider the potential hazards and who the most "talkative" employees are.

1 blog.trendmicro.com

In 88 percent of cases, employees who enter into correspondence do not work in IT (instead, they are mostly accountants, lawyers, or managers). One in four employees who responded to a suspicious email was a team supervisor. Although information security staff were a minority of responders (3%), even they were not immune, proving that social engineering is a powerful tool for attackers and even security-savvy employees can slip up.



Breakdown of phishing-susceptible employees, by occupation

What do employees normally write in response to an unusual email?

Most often, the recipient informs that the link or attachment would not open. Checking the event log on the data collection server used for testing, the experts saw that the recipient had clicked the phishing link several times, entered different password variations, and tried the passwords used for other services. In some cases, users made 30 to 40 attempts!

Sometimes users wrote "You are writing to the wrong person" and proposed other addressees.

So what is the problem? As soon as an attacker is sure that an employee considers him or her a colleague, further exchange of communications will be aimed at teasing out required information without raising any suspicions: software version, antivirus protection, email addresses of other employees, mobile phone numbers, or the company organizational chart, for example. In short, any valuable information that could be used for planning and conducting subsequent attacks.

In some cases, employees unwittingly go the extra mile to help an attacker: they forward an infected email message to colleagues with a request to "open the attachment" or "click the link." Such cases were observed in our testing. At one client company, employees received test messages with an attached file *Vacation_schedule.xls*, which they could not open. They forwarded the message to the IT department with a request to help open the file, IT staff opened the message and ran the file, apparently considering their colleague (whom they knew personally) to be a trusted source.

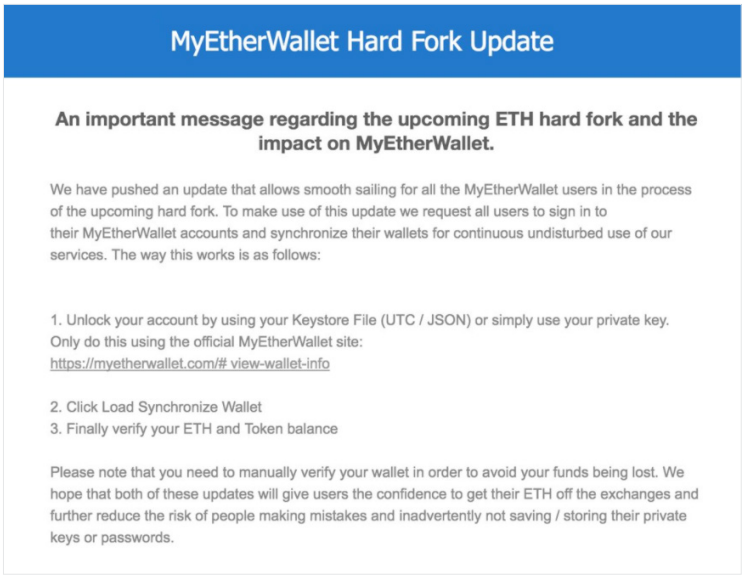
Even though messages were sent to pre-defined groups based on prior agreement with the client, we were surprised to discover that the files were downloaded and run by entirely different people who were not in these groups. As it seems, employees started to spread the message (and attachment) amongst themselves. A message could make it all the way to the workstations of system administrators and security specialists, who were not among the intended recipients.

Another important factor is the response of corporate security departments. In cases when the client's information security team had not been warned in advance, only two companies managed to quickly detect and filter the phishing emails, as well as block attempts to go to a phishing resource.

IT ALL COMES DOWN TO TRUST

For testing purposes, Positive Technologies experts registered domains that are similar in spelling to the domains of the clients. This trick is often used by real attackers, who hope that victims will overlook an incorrect spelling, prefix, or postfix. Generally speaking, only people well versed in IT use publicly available web services[2] to check if a domain name belongs to a company. Sometimes it is truly difficult to catch a copycat (if the attacker is using the real domain name of a company or trusted partner). But other times malicious messages are sent from an obviously fake domain name, such as admin@excamplle.com. In these cases, compromising is the result of simple carelessness or complete ignorance of security.

In October 2017, hackers sent phishing messages[3] that claimed to come from the administration of MyEtherWallet, a popular online cryptocurrency wallet. According to the messages, a website update was in process and user accounts had been blocked. Users were asked to click a link in the message to sign in and verify their balance.



MyEtherWallet Hard Fork Update

An important message regarding the upcoming ETH hard fork and the impact on MyEtherWallet.

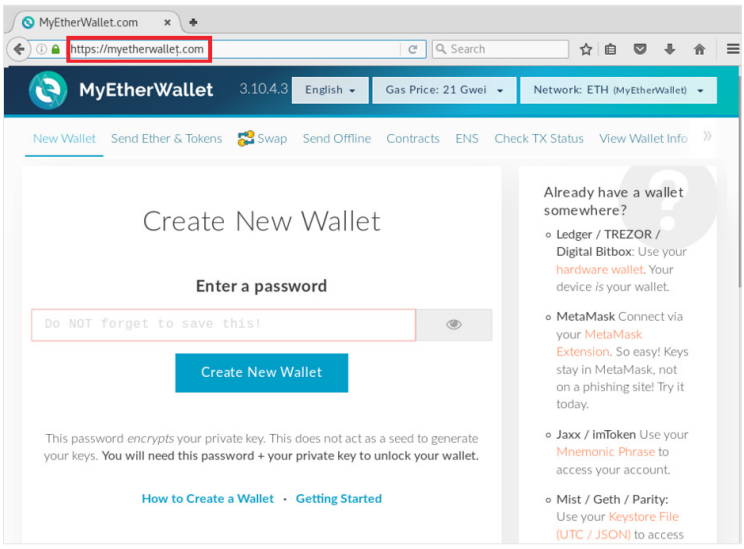
We have pushed an update that allows smooth sailing for all the MyEtherWallet users in the process of the upcoming hard fork. To make use of this update we request all users to sign in to their MyEtherWallet accounts and synchronize their wallets for continuous undisturbed use of our services. The way this works is as follows:

1. Unlock your account by using your Keystore File (UTC / JSON) or simply use your private key. Only do this using the official MyEtherWallet site:
https://myetherwallet.com/# view-wallet-info

2. Click Load Synchronize Wallet
3. Finally verify your ETH and Token balance

Please note that you need to manually verify your wallet in order to avoid your funds being lost. We hope that both of these updates will give users the confidence to get their ETH off the exchanges and further reduce the risk of people making mistakes and inadvertently not saving / storing their private keys or passwords.

The link led to a website identical to the real myetherwallet.com. The only difference was in the last character, where instead of "t" the attackers used "ţ", an almost identical Unicode character.

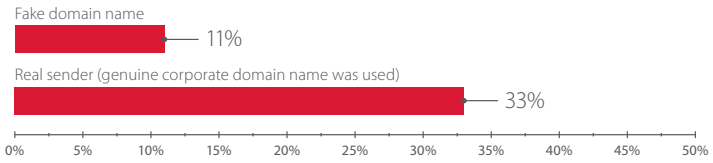


2 whois.com/whois/

3 dearbytes.com/blog/cryptocurrency-phishing/

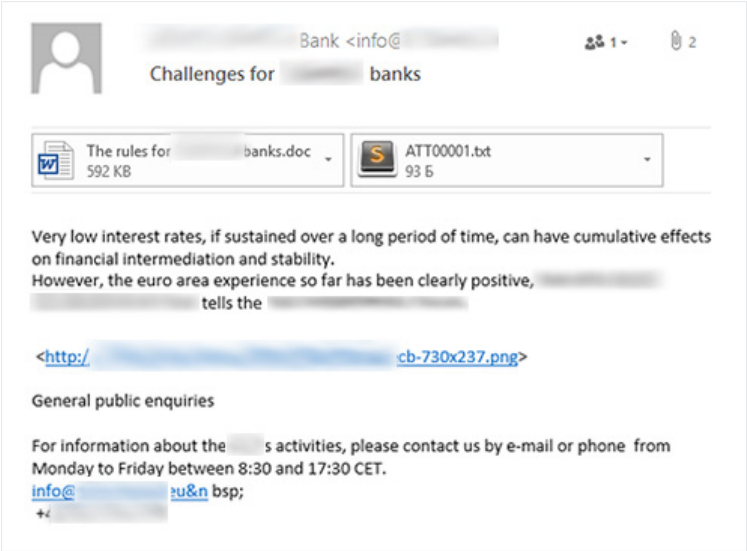
Apart from obscure Unicode symbols, methods for hacker subterfuge can include adding a dash to a real domain name, substituting letters that look or sound similar, or adding prefixes and postfixes. However, we believe that this technique will fade away as common users become more security-savvy.

The results of our tests prove this point: 33 percent of recipients performed a risky action only if the email was from a real sender (one using the actual domain name of some company). With a fake domain name, such cases were less frequent and only 11 percent of employees took the messages at face value.



Type of sender

This fact explains the value of Business Email Compromise for attackers, who eschew fake domains and prefer to avoid suspicion by sending emails that appear to come from business partners. The Cobalt[4] group, for example, used phishing emails as an initial vector for infrastructure infection. In addition to using fake domain names, the attackers also sent emails from real domains belonging to banks and systems integrators. The attackers had previously hacked the infrastructures of those companies for this purpose. Since colleagues, contractors, and partners tend to write during the regular working day, the attackers sent their malicious emails during the victims' business hours to appear more plausible.



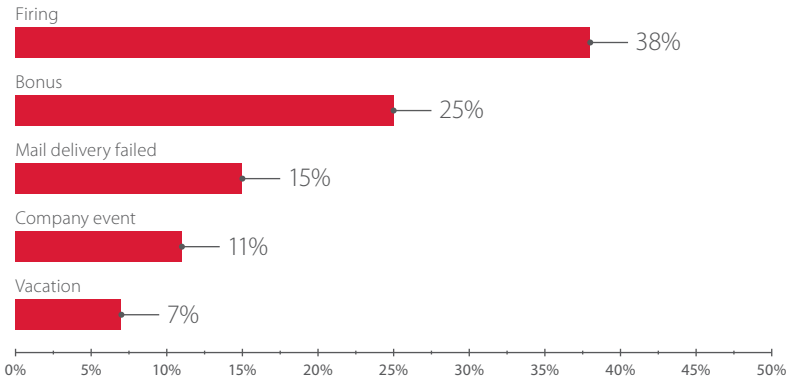
A GOOD SUBJECT LINE IS ALL IT TAKES

Attackers take advantage of fear, greed, hope, excitement, or any other imaginable emotion to trick recipients into ignoring their better judgment. When someone suddenly receives an email with the subject line "Mail Delivery Failed: employee termination list," elementary cybersecurity rules fly out the window—the user does not even start wondering why he or she received a notification about an undeliverable message.

The subject is often the reason that compels an employee to open a letter, click a link, or download and run a file without stopping to wonder who sent the message and why the domain is written strangely. During testing, the experts carefully created a suitable subject line and text for each client scenario.

If not read carefully, these messages are difficult to distinguish from legitimate ones. The following diagram shows the most effective phishing emails used in client scenarios.

4 ptsecurity.com, PDF



Effective phishing scenarios

Unsurprisingly, the fear of being fired is enough of a jolt to forget about security: almost 40 percent (!) of phishing messages with a dismissal-related subject line made users act insecurely. Emails with such words as "bonus", "reward", and "wage increase" also demonstrated a high rate of success, at about one in four users. Attackers may also make reference to some event, such as a holiday or office party. 11 percent of test messages with such subject lines prompted unsafe actions by users.

CALL MY NAME AND I'LL BE THERE

Although email is the most common and effective social engineering method, being both scalable and simple, it is not the only technique used by attackers. They can make phone calls and claim to be from technical support. They try to obtain information from the employee or trick the employee into clicking a malicious link, entering a password, or downloading and running a malicious file. A classic example: an attacker calls early Sunday morning and asks the employee to come to the office as soon as possible. But as the conversation continues, it "luckily" turns out that the victim can simply give his or her account password so the support staff can deal with it on their own. The victim willingly parts with the password, thanking the attacker all the while.

As compared to phishing mailings, which can be quick, large-scale, and received near-simultaneously by victims, phone calls can be a drag: attackers have to prepare and spend time on each call. And calling all company employees would certainly attract attention. Experts made phone calls to the employees who responded to email messages, if these employees either gave their phone number during subsequent correspondence or if their email signature contained such information. This information allowed for making calls with high precision to users who were eager to communicate and help solve the "problem" indicated by the tester. As a result, this attack vector was highly effective. In the course of phone conversations, 44 percent of employees gave out their passwords, told about the software versions installed, and clicked a certain link.

The test ran as follows: after an employee answered a phishing email, our experts obtained permission from the client and then called that employee, claiming to be from technical support. They spelled out the name of a fake corporate website (similar to the real domain name, but containing a hyphen). The victim was unable to log in successfully and the following dialog took place:

[PT expert]: Let's do it this way: you give us your password, and we will do everything on our own.

[Employee]: Oh, that's even better. My password is 978654321#!

[PT expert]: OK, thank you.

[Employee]: Please don't change it, it's so convenient!

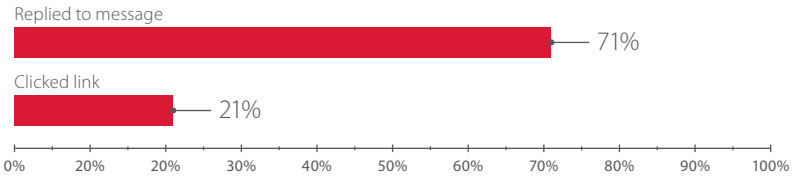
In some cases employees asked for the caller's name, and our experts said their real names. The most vigilant employees checked to see if there was such an employee at the company; when they could not find such a person, they disconnected. Naturally, an attacker can find out such information in advance by combing social networks or other websites where employees disclose their positions and contact information. Such basic preparations would surely make these attacks more successful.

One of the reasons why employees refused to comply was corporate regulations: an employee refused outright to click a link, because "that's not the way we do things." In such a case, we can only praise employees for diligence and commend the client for its security culture. In some cases, users asked whether it was safe to click the link. Despite their doubts, they clicked the link and even entered their credentials.

FACEBOOK FOR THE WIN

Attackers know how to use social networks. A victim's profile on a social network can be an effective tool for them. For example, an attacker could infect an employee's device via a social network, knowing that this device will be used to connect to the company's intranet or check work emails. Users with poor security awareness may use social networks to discuss business issues or send confidential documents, which can be highly valuable for attackers. Sometimes users have the same password, or very similar passwords, for social networks and work accounts. Any data the attacker manages to obtain can be used to attack corporate infrastructure. Nowadays, this method is widely applied by cybercriminals. One example is the SongXY hacker group, which participated in attacks against industrial companies and government institutions in CIS countries in 2017. The attackers surfed social networks for profiles of employees and sent messages to them. Another benefit for attackers is that users frequently log in to social networks from office computers. So opening a malicious link may give an attacker direct access to the company's intranet.

Our testing included interaction with client employees via social networks. Experts identified employees whose profile indicates their current employer. The client then edited this list to remove fake accounts and former employees. Messages were sent only to people expressly approved by the client. To measure the success rate, experts used a simple logger that records whether the recipient clicked a link leading to a specially created website. More than 70 percent of employees replied eagerly, while 21 percent opened the link sent to them.



Risky behavior of employees on social networks

In a real attack, potential methods include social networks and instant messaging clients. Therefore, whenever employees indicate their place of work on a social network, they should be fully aware of their responsibility to keep their guard up both on and off the job.

CONCLUSION

Phishing is a perennial method used by hackers against both common users and corporate infrastructures due to its cheapness, simplicity, and high effectiveness.

The best recommendation for common users is to be always on alert. Check who the sender is before clicking a link or opening attachments to make sure that they are not malicious. Before opening a file, scan it with antivirus software. If available at the workplace, open files in a special sandbox. Make sure that the sender's domain is legitimate. In case of any doubts, use an alternative method to communicate with the sender, such as instant messenger or phone, to check whether an email message and its associated domain are legitimate. Compliance by employees with these simple recommendations during attacks by the Cobalt group would have saved banks from millions in losses.

IT and information security teams can apply a number of simple measures to enhance protection from phishing email attacks. A properly configured SPF record prevents forgery of emails sent from the company's domain. This technology verifies the sender's server. For best results, also use DKIM, which sets a signature for confirming the authenticity of the address in the "From" field, and DMARC, which minimizes incoming phishing emails by applying rules on the recipient's server to identify the sender's domain. A PTR record can be used as additional protection to look up an IP address and identify the sender's host, as well as check spam databases for the sender's IP address.

It is recommended to block delivery of email attachments with extensions that are used in executable (.exe, .src), system (.dll, .sys), script (.bat, .js, .vbs), and other files (.js, .mht, .cmd). Files having any of these extensions may contain malicious code placed by an attacker in a phishing email. Read this research[5, 6] for a more detailed list of such extensions. We also recommend deploying an on-demand malware detection system so that employees can send email attachments or any other files for scanning at any time. Corporate antivirus software can detect malicious links and files in emails before a user ever sees (or clicks) them. However, if an attacker applies obfuscation, antivirus software may fail to detect malware immediately. Therefore it is recommended to perform scanning both immediately before opening a file and retrospectively. Retrospective detection can still offer valuable information: the fact of system compromise, compromise date, infection source, incident localization, and other data needed for a more thorough investigation. Timely attack detection and interdiction can prevent serious consequences. In addition, the importance of installing application and OS updates in a timely manner cannot be overestimated—otherwise, systems are left vulnerable to a long list of security flaws.

On an organizational level, companies should start by developing and implementing a program for improving the information security awareness of employees. Training must be periodic and followed by testing of every employee. The emphasis of training should be on practical aspects of security and reminding that every employee, even if "non-technical," has security responsibilities. A positive sign is when employees inform corporate security of suspected phishing emails, especially if a message has clearly been created with great care. With this cooperation, even if an infection or data leak has already occurred, security staff can promptly start response and mitigation.

5 blueteamer.blogspot.ru/2017/05/
6 support.office.com

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com