



How to Spot Phishing Attacks and Defend Your Business against Them

Austin Technology
3/52 Frobisher St
Osborne Park, WA, 6017

t: 1300 787 429

w: www.austintechnology.com.au

About This White Paper

Businesses are under assault. Organizations are increasingly becoming the target of phishing attacks, which are growing in sophistication and number. These attacks are taking their toll on the bottom line. The total estimated losses from phishing totalled \$1.3 billion in the United States, \$160 million in Canada, and \$130 million in the United Kingdom in 2015 alone.

Given the prevalence and serious financial consequences of phishing attacks, you need to take action. You need to develop a sound strategy that will protect your business against this threat.

In this white paper, you will learn:

- What phishing is
- How to spot phishing attacks
- What spear phishing is
- How to spot spear phishing attacks
- How a three-pronged approach can help you defend against both types of attacks

After growing in number and sophistication over the past two decades, phishing attacks have become a serious threat to businesses. The statistics are staggering:

- A phishing scam is detected every minute.¹
- In 2015, 85 percent of organizations worldwide reported experiencing phishing attacks, with 60 percent noting an increase in the number of attacks received compared to the previous year.²
- The total estimated losses from phishing totalled \$1.3 billion in the United States, \$160 million in Canada, and \$130 million in the United Kingdom in 2015 alone.³

Given the prevalence and serious financial consequences of phishing attacks, your business needs to address this threat. To do so, you need to not only understand what phishing is but also know about its equally troublesome offshoot, spear phishing. Even more important is knowing how to spot both types of attacks. Armed with this knowledge, you can develop a sound strategy to defend your business against phishing and spear phishing threats.

What Is Phishing?

Phishing is a form of fraud in which cybercriminals masquerade as a reputable person or a legitimate organization. They often try to obtain sensitive information, such as login credentials or account information. They then use this information to steal money, data, and even people's identities.

Cybercriminals execute phishing attacks through various communication channels, including phone calls, instant messaging, and Short Message Service (SMS) messaging. However, the most common channel is email messages, as it enables cybercriminals to attack a massive number of people at once. Cisco Systems reports that in a typical phishing attack, emails are sent to about 1 million people.⁴

In a typical phishing attack, emails are sent to about 1 million people.

In email phishing scams, cybercriminals use a convincing pretence to lure recipients into performing an action. These digital con artists usually want the recipients to click a link or open an attachment. Doing so often unleashes malware.

The phishing email itself is harmless. Recipients can simply delete it to avoid becoming a victim. However, if they fall for the scam or inadvertently click the link or open the attachment, they might release one of many different types of malware. For example, the malware might be a web Trojan that collects credentials from victims' computers, a key logger that tracks input from their keyboards, or ransom ware that encrypts and holds their files for ransom.

¹ RSA Online Fraud Resource Center, [Current State of Cybercrime](#)

² Wombat Security Technologies, "[State of the Phish 2016](#)"

³ RSA Online Fraud Resource Center, [Total Global Losses from Phishing Attacks \(2015\)](#)

⁴ Cisco Systems, "[Email Attacks: This Time It's Personal](#)"

How to Spot Phishing Attacks

A key defence against phishing attacks is learning how to spot them. Are you able to spot a phishing email? Take a look at the following:

From: Chase Bank US <alert-id.7437712327-vl@dynamicalert.hu> Sent: Mon 2/22/2016 12:18 PM
To: JaneDoe@ABCservices.com
CC:
Subject: CHASE Alerts! 02/22/2016 - e-mail no: 7437712327/VL

ACCOUNT ALERT!

Dear JaneDoe@ABCservices.com,

Due to an unusual number of failed login attempts, your online banking access has been temporarily suspended. <http://dynamicalert.hu/upload/22feb743aca/index.php>
Ctrl+Click to follow link

To restore your account access please click: <https://chaseonline.chase.com>


IMPORTANT NOTE:

If we do not receive the appropriate account verification within 24 hours, you will need to visit a CHASE branch to restore your account access.

Sincerely,
Chase Bank Online

Is this a legitimate email or a phishing scam? What about this one:

From: PayPal <admin@secure-paypal.com> Sent: Wed 2/10/2016 4:30 PM
To: JaneDoe@ABCservices.com
CC:
Subject: Receipt for Your Payment to SMB Office Supply Deliveries

 Feb 10, 2016
Transaction ID: 12CZ526791278474UK22

Hello,

You sent a payment of \$496.21 USD to SMB Office Supply Deliveries (paypal@smbofficesupplydeliveries.com)

It may take a few moments for this transaction to appear in your account.

Merchant SMB Office Supply Deliveries paypal@smbofficesupplydeliveries.com	Instructions to merchant You haven't entered any instructions.
Shipping address - unconfirmed United States	Shipping details The seller hasn't provided any shipping details yet.

Description	Unit price	Qty	Amount
Multiuse Copy Paper, 8 1/2" x 11", 8-Ream Case	\$46.99 USD	10	\$469.90 USD
	Subtotal		\$469.90 USD
	Tax		\$26.31 USD
	Total		\$496.21 USD
	Payment		\$496.21 USD

Payment sent to paypal@smbofficesupplydeliveries.com

Issues with this transaction? <https://www.secure-paypal.com>
Ctrl+Click to follow link

If you haven't authorized this charge, open a dispute at <https://www.paypal.com/resolutioncenter> to get a full refund.

If you were unsure about one or both of these emails, do not feel bad. It is much easier to spot a phishing email if you know what to look for.

What to Look for in an Email

An email might be a phishing attack if it contains one or more of the following elements:

A generic greeting. When cybercriminals send out phishing emails, they send them out to the masses. As a result, they often start the emails with a generic greeting, such as "Dear member" or "Dear Acme Bank customer". Another way cybercriminals avoid personal greetings is to use the recipient's email address as the greeting ("Dear JaneDoe@ABCservices.com") or just include a simple "Hello". They might not even include a greeting.

A deceptive email address. Phishing emails sometimes include a deceptive email address in the "From" field. For example, a cybercriminal might send out an email message using the address "promotions@amazon.com" instead of the real "@amazon.com" address. Deceptive email addresses increase the chance of someone falling for the scam.

Misspellings or grammatical errors. Many phishing emails come from cybercriminals in foreign countries, so they might contain misspellings and grammatical errors. Plus, intentional misspellings can sometimes help get emails past spam filters.

A request to update or verify information. The goal of most phishing attacks is to get sensitive information.

Cybercriminals like to do this by posing as a popular legitimate financial institution (e.g., a bank) and asking you to update or verify your information. If an email asks you to update or verify your password, credit card number, or bank account number, it is most likely a scam.

A sense of urgency. A common tactic to get you to fall for a phishing scam is to create a sense of urgency. The cybercriminals first let you know about a problem that requires your attention. Then, they let you know that there will be unfortunate consequences if you do not take action quickly. For instance, an email supposedly from a service provider might say that your credit card on file has expired and if you do not update it in the next 48 hours, you will experience a disruption in service.

Deceptive URLs. Many phishing emails include deceptive URLs. The URL or linked text that is displayed might be legitimate, but when you hover your mouse cursor over it (without clicking it), you might discover that the actual URL does not match the displayed information. These deceptive links can lead to spoofed (i.e., fake) websites that try to get your sensitive information or sites that will install malware on your computer.

An attachment. Phishing emails sometimes use attachments rather than deceptive links to install malware on computers. Many different types of files can contain malicious code, including Adobe Portable Document Format (PDF) files, Microsoft Word (DOC and DOCX) documents, and executable (EXE) files. Legitimate organizations typically do not email files out of the blue. So, unless you specifically requested a document from an organization, be wary of any attachments supposedly emailed by one. Similarly, be wary of attachments emailed by individuals if you did not request the file.

A common tactic to get you to fall for a phishing scam is to create a sense of urgency — act now or pay the consequences.

A notice about winning a prize. Although they are not as common as they used to be, you might still encounter phishing emails that inform you about a lottery or contest you won. To claim it, the cybercriminals usually ask you to pay a processing fee as well as provide some sensitive information.

Preying on people's compassion, cybercriminals often send out phishing emails that pretend to be collecting donations for the victims of a disaster.

A request for a donation. Preying on people's compassion, cybercriminals often send out phishing emails that pretend to be collecting donations for the victims of a disaster. One of the most well-known cases occurred after Hurricane Katrina.⁵ Cybercriminals sent out phishing emails asking recipients to donate to the Red Cross relief effort. Email links took the victims to various websites that looked like legitimate Red Cross donation pages. However, cybercriminals created these spoofed websites for the sole purpose of stealing donors' credit card numbers, PayPal passwords, and other sensitive information. The American Red Cross reported finding more than 15 of these bogus websites.

Take a Second Look

Knowing the types of elements to look for makes it easier to spot phishing emails. For instance, based on these elements, it is evident that both the Chase Bank and PayPal emails shown previously are phishing scams. The Chase Bank email is an example of a less refined phishing attack. There are numerous signs indicating that it is a scam, as the following shows:

The image shows a screenshot of a phishing email with several red callout boxes pointing to suspicious elements:

- From:** Chase Bank US <alert-id.7437712327-vl@dynamicalert.hu> (Callout: "Email address clearly not a Chase Bank address")
- To:** JaneDoe@ABCService (Callout: "Spelling error")
- Subject:** CHASE Alert! 02r22220... (Callout: "Spelling error")
- Body:** ACCOUNT ALERT! Dear JaneDoe@ABCServices.com, (Callout: "Email address instead of name")
- Body:** Due to an unusual number of failed login attempts, your online banking access has been temporarily suspended. (Callout: "http://dynamicalert.hu/upload/22feb743aca/index.php Ctrl+Click to follow link")
- Body:** To restore your account access please click: <https://chaseonline.chase.com> (Callout: "Actual URL is different from the displayed URL")
- Body:** IMPORTANT NOTE: (Callout: "Note trying to create a sense of urgency")
- Body:** If we do not receive the appropriate account verification within 24 hours, you will need to visit a CHASE branch to restore your account access. (Callout: "Bank name sometimes in all capital letters")
- Body:** Sincerely, Chase Bank Online (Callout: "Bank name sometimes in all capital letters")

Besides using the email address in the greeting, there is a spelling error as well as inconsistencies in how the bank name is presented. The biggest red flags, though, are the email address in the "From" field and the actual URL. Both include ".hu" in the domain name, which indicates that the domain is in Hungary. This is very suspicious since the domain is supposedly for a bank located in the United States.

⁵ Avast Software, "[High potential for Hurricane Sandy internet scams](#)"

The PayPal email is a more sophisticated phishing attempt. It looks like a real PayPal receipt, except for a few details, as the following shows:

The screenshot shows an email header with the following fields: From: PayPal <admin@secure-paypal.com>, To: JaneDoe@ABCservices.com, CC: (empty), Subject: Receipt for Your Payment to SMB Office Supply. A red callout box points to the 'From' field, stating 'Email address not a legitimate PayPal address'. The email body features the PayPal logo, the date 'Feb 10, 2016', and a transaction ID '12CZ526791278474UK22'. The greeting is 'Hello,' with a red callout box stating 'Name missing'. The main text reads: 'You sent a payment of \$496.21 USD to SMB Office Supply Deliveries (paypal@smbofficesupplydeliveries.com)'. Below this, it says 'It may take a few moments for this transaction to appear in your account.' The email contains two columns of information: 'Merchant' (SMB Office Supply Deliveries, paypal@smbofficesupplydeliveries.com) and 'Instructions to merchant' (You haven't entered any instructions.). Another column shows 'Shipping address - unconfirmed' (United States) with a red callout box stating 'Address missing', and 'Shipping details' (The seller hasn't provided any shipping details yet.). A table follows with columns for Description, Unit price, Qty, and Amount. The table lists 'Multiuse Copy Paper, 8 1/2" x 11", 8-Ream Case' with a unit price of \$46.99 USD, a quantity of 10, and an amount of \$469.90 USD. Below the table, a summary shows Subtotal (\$469.90 USD), Tax (\$26.31 USD), Total (\$496.21 USD), and Payment (\$496.21 USD). At the bottom, it states 'Payment sent to paypal@smbofficesupplydeliveries.com'. A section titled 'Issues with this transaction?' includes a red callout box stating 'Actual URL is different from the displayed URL' pointing to a link 'http://www.secure-paypal.com Ctrl+Click to follow link'. Below this, it says 'If you haven't authorized this charge, open a dispute at https://www.paypal.com/resolutioncenter to get a full refund.'

One detail is the greeting, which just says "Hello". The greeting on a real PayPal receipt will include either the individual's full name or the business's name, depending on how the account is set up. Also missing is the business's address, which is suspicious. How can the office supplies be delivered to that business if there is no address?

Another problem with this email is that it contains a deceptive email address in the "From" field as well as a deceptive URL. The deception is not immediately obvious, as they both include "PayPal" in the domain name. However, a quick Internet search reveals that "secure-paypal.com" is a known fake PayPal address.⁶

⁶ PayPal, "[Recognize fraudulent emails and websites](#)"

What Is Spear Phishing?

Like phishing ploys, spear phishing scams are designed to obtain sensitive information and are typically sent via email. However, cybercriminals send a lot fewer emails because spear phishing scams take a more personalized approach.

In a traditional phishing attack, the digital con artist sends a one-size-fits-all email to the masses. For this reason, the phishing emails use a generic greeting and text. In a spear phishing attack, the con artist targets specific individuals and personalizes the emails sent to them. The emails typically include the target's name in the greeting and present the call for action in a context that makes sense to the recipient.

In a recent spear phishing attack, cybercriminals included the recipients' home addresses. People who fell for the scam had their computers infected with ransomware.

In a recent spear phishing attack, cybercriminals even included the recipients' home addresses, which authorities believed they obtained from publicly available databases. The people who fell victim to the scam and opened the attached file had their computers infected with ransom ware.⁷

Organizations are the targets of most spear phishing attacks. Cybercriminals often send spear phishing emails to employees, trying to get them to visit a deceptive website or open a malicious attachment that installs malware. Sometimes the targets are executives or other powerful members of an organization, in which case the scam is referred to as whaling.

To personalize the emails, cybercriminals will try to get information from organizations' websites and social media networks, such as LinkedIn and Facebook. Plus, Internet searches can provide information about not only the intended targets but also the lingo and common processes used in the industry in which the targets work. Cybercriminals sometimes even call organizations to obtain names, titles, and email addresses. Using the information they find, they will try to create a compelling email that will not raise any suspicions about it being a scam.

The additional effort to personalize the emails pays off, according to research by Wombat Security Technologies.⁸ In simulated attacks, Wombat discovered that phishing emails with personalized greetings had click-through rates 17 percent higher than those with no personalization.

How to Spot Spear Phishing Attacks

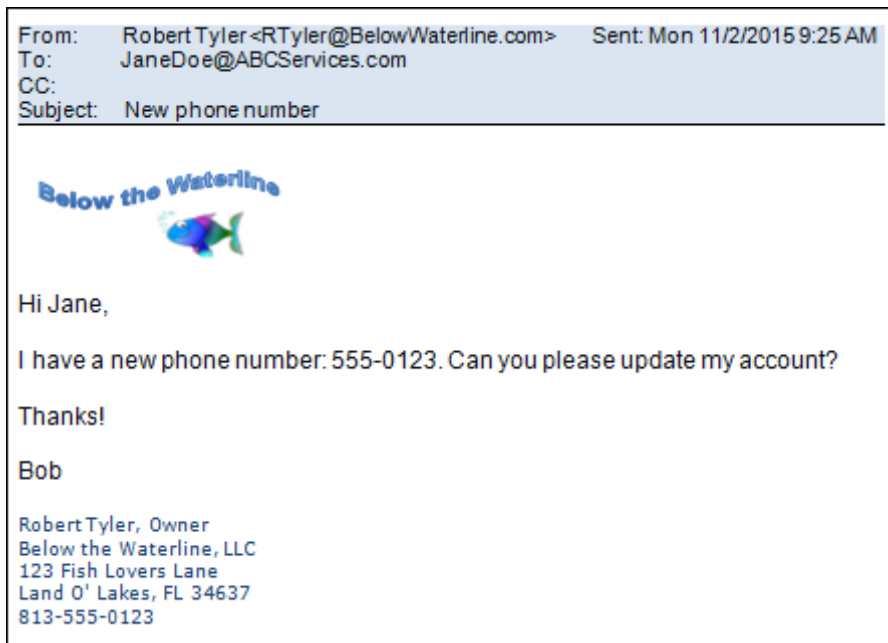
Spear phishing emails are more sophisticated, so they are harder to spot. Cybercriminals take the time to research their subjects and craft their messages, so many of the tell-tale signs of a phishing email do not apply. Since spear phishing emails usually target organizations, they rarely talk about winning the lottery or donating money. Nor do they contain a generic greeting. Instead, the greeting typically includes the name of the intended victim. Misspellings and grammatical errors are the exception rather than the norm. Plus, the emails take on a softer, business-like tone rather than trying to instil a sense of urgency.

⁷ ZDNet, "[Meet the new ransomware that knows where you live](#)"

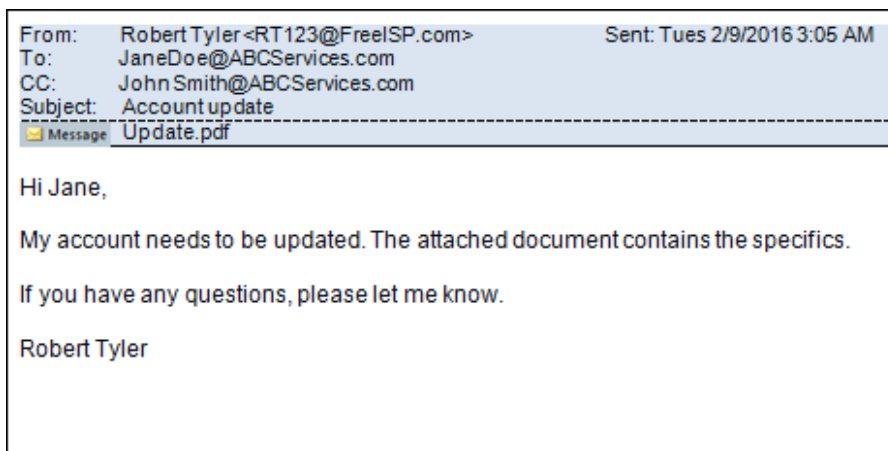
⁸ Wombat Security Technologies, "[State of the Phish 2016](#)"

Despite the lack of these tell-tale signs, there are some elements that might indicate an email is a spear phishing attack. Like their phishing counterparts, spear phishing emails try to get employees to perform an action. For example, an email supposedly from a supervisor might ask the targeted employee to review some updated procedures, which are in an attached malware-laden file. Besides attachments, spear phishing emails might include deceptive email addresses and deceptive links.

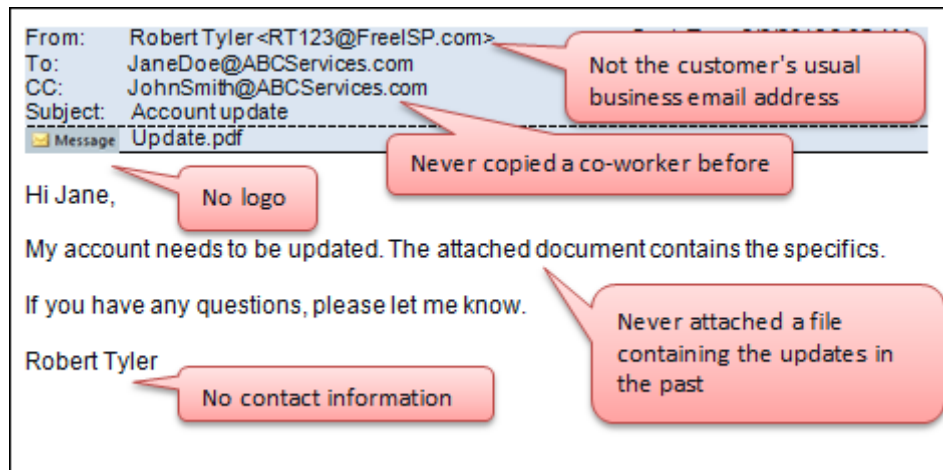
Another way to spot spear phishing emails is to pay attention to details. The best way to illustrate this is with an example. Suppose that one of Jane Doe's regular customers emails her whenever he needs something updated in his account. For example, here is a typical email asking her to update his phone number:



Several months later, Jane receives another update request:



Based on past emails, though, she is suspicious of the request. Besides the more formal tone, she notices other differences:



A quick call to the customer confirmed her suspicion that he did not send the email. Jane's attention to detail thwarted the spear phishing attack.

A Three-Pronged Strategy to Defend against Phishing and Spear Phishing Attacks

To help your company defend against phishing and spear phishing attacks, you need a sound strategy. If you do not already have one in place, you might consider using a three-pronged approach. First, try to stop as many phishing and spear phishing emails as you can from reaching employees. Second, educate employees and executives alike about these types of attacks. Finally, take measures to help mitigate the effects of scams should someone inadvertently fall for one.

1. Stop the Emails before They Reach the Employees

More than 6 billion phishing emails are sent worldwide each month, according to Dell SonicWALL.⁹ You can stop many of these phishing and spear phishing emails from reaching your employees if you:

- Keep email filtering tools up-to-date. These tools use various filters to help weed out phishing emails and other types of spam. Most email programs include filtering tools, but you can also purchase advanced filtering solutions.
- Use anti-malware software. It can help catch emails that include malicious attachments.

⁹ Dell SonicWALL, "[Phishing Facts](#)"

2. Educate Employees

Educating employees about phishing and spear phishing is crucial given that some attacks will likely reach their email inboxes. Topics that you might consider covering in your employee training program include the following:

- The similarities and differences between phishing and spear phishing
- The elements commonly found in phishing and spear phishing emails so that employees are better able to spot them
- The risks associated with clicking an email link or opening an email attachment, especially if the email is from an unknown source
- How to check for deceptive links in emails by hovering the mouse cursor over them (but not clicking them)
- What employees should do if they suspect an email is a scam (e.g., simply delete it, notify someone about it)
- The dangers of providing personal or company information to people who should not have access to it

After the employees have completed the training program, you might want to send out fake phishing or spear phishing emails to them to see if they fall for the scam.

After the employees have completed the training program, you might want to send out fake phishing or spear phishing emails to them to see if they fall for the scam. This test can reinforce what employees have learned as well as help determine the effectiveness of the training.

3. Take Measures to Mitigate the Effects of Successful Attacks

Despite your best efforts to keep phishing and spear phishing emails from reaching employees and educating staff on how to spot them, someone might fall for a scam. Taking a few pre-emptive measures might help mitigate its effects:

- Keep operating systems and applications (e.g., Adobe Reader, Java) up-to-date. Cybercriminals often exploit known vulnerabilities in software to carry out their phishing and spear phishing attacks. By making sure your software has the latest security patches, some malicious code unleashed by an attack might be stopped in its tracks.
- Use a unique strong password for each business account. Obtaining login credentials is the goal of many phishing and spear phishing scams. If cybercriminals get the password for one account, they will try to use that password (or a similar version of it) to access other accounts. If you use a unique strong password for each business account, they will not be able to use the compromised password to access other accounts.
- Perform backups regularly and make sure they can be successfully restored. If the malware unleashed by a scam wreaks havoc in your IT environment (e.g., ransom ware released through a spear phishing scam), you can restore your systems and data from backups taken before the attack.

Now Is the Time to Take Action

Phishing and spear phishing are here to stay. As long as people keep falling for these scams, they will be the weapon of choice for many cybercriminals. Thus, you need to take steps to defend your business against these threats.

If you do not have a plan in place, you can use the three-pronged approach presented here as a possible starting point. We can help you determine the specific steps that you should take to protect your business against phishing and spear phishing attacks.