Vade Secure
Predictive Email Defense

SPEAR PHISHING:

The Targeted Attacks That Aim for Your Business

TABLE OF CONTENTS

WHAT IS SPEAR PHISHING?

A form of social engineering, spear phishing is a malicious email that impersonates an individual for the purpose of tricking a recipient into completing a desired action—typically financial in nature. Often, a hacker will impersonate a victim's acquaintances, such as colleagues, executives, clients, or vendors.

> **Spear phishing cost US businesses $1.7 billion in 2018**
> *- FBI Internet Crime Report 2019*

THE CONTINUUM OF EMAIL SPOOFING

To trick recipients into thinking they're reading an email from a trusted sender, spear phishers use a technique called "spoofing" that allows them to impersonate a legitimate sender and email address. There are three primary methods of email spoofing:

Display Name Spoofing: Display name spoofing impersonates the sender's name but not the email address. This is effective because many users will trust the sender immediately upon seeing the name. It's also effective because many email clients, especially on mobile, show only the sender's name but not the email address.

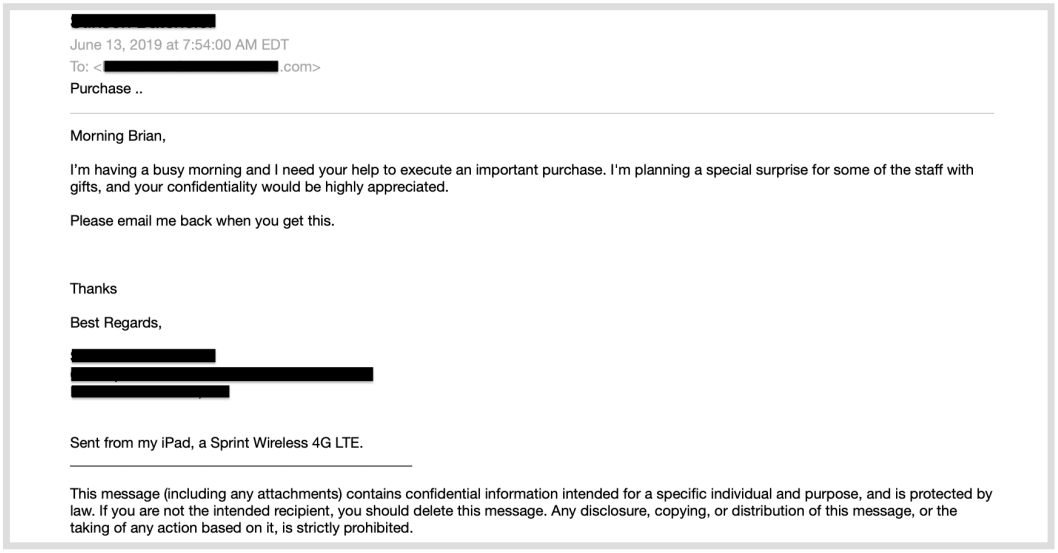
Domain Spoofing: This method is more sophisticated than display name spoofing but also easier to detect by SPF (Secure Policy Framework), DMARC (Domain Message Authentication Reporting), and DKIM (Domain Keys Identified Email). With domain spoofing, a spear phisher can specify the email address they want to spoof. When an email address is an exact replica of a trusted sender, users are unlikely to recognize that the email is spoofed.

Close Cousin: A close cousin email address is nearly identical to a legitimate one, with only a slight modification. In the past, close cousin spoofing attempts were more obvious, such as mIcrosoft.com instead of microsoft.com. Today, attempts are more advanced and difficult to spot, such as user@mycompanyltd.com instead of user@mycompany.com. These subtle changes can be extremely difficult to spot for busy staff who quickly read and respond to emails, especially when they are urgent in nature. Moreover, DMARC and SPF are ineffective against close cousins because they only protect exact domains.

SPEAR PHISHING VS PHISHING

Spear phishing and phishing attacks both leverage impersonation to commit fraud. The difference between the two is that spear phishing emails impersonate people, while phishing emails impersonate brands. Unlike phishing, spear phishing targets a single individual, includes no links or attachments in the email, and typically features a request for a wire transfer, gift cards, or direct deposit change, rather than account credentials.

Spear Phishing


[redacted]
June 13, 2019 at 7:54:00 AM EDT
To: <[redacted].com>
Purchase ..

Morning Brian,

I'm having a busy morning and I need your help to execute an important purchase. I'm planning a special surprise for some of the staff with gifts, and your confidentiality would be highly appreciated.

Please email me back when you get this.

Thanks

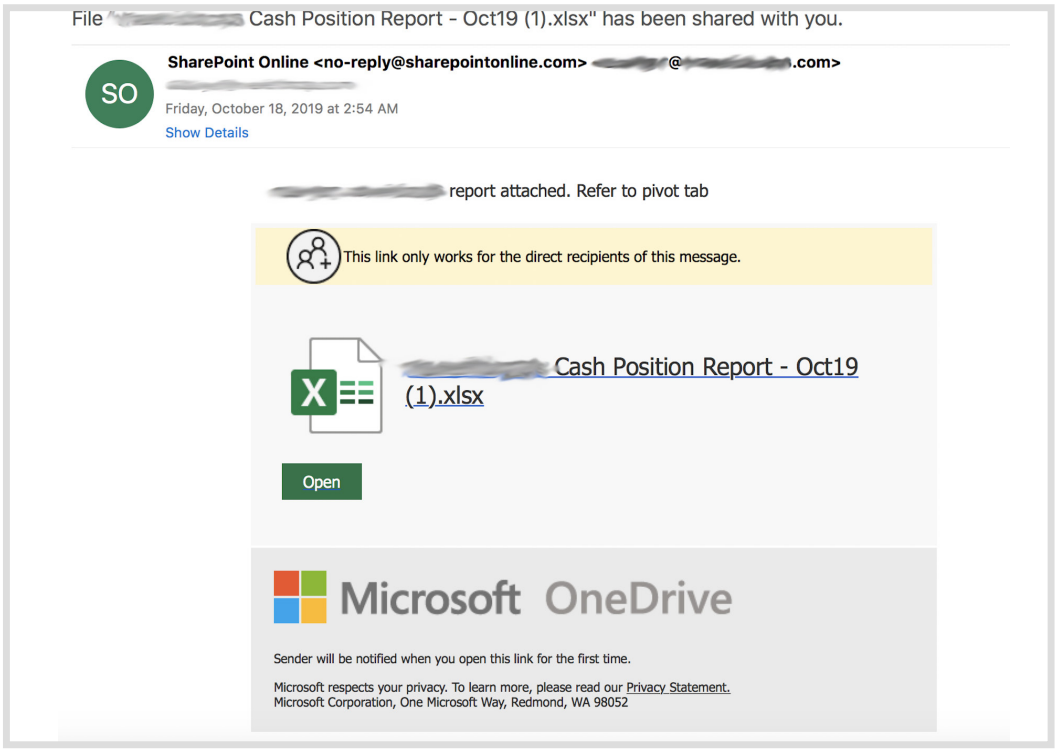
Best Regards,

[redacted]

Sent from my iPad, a Sprint Wireless 4G LTE.

This message (including any attachments) contains confidential information intended for a specific individual and purpose, and is protected by law. If you are not the intended recipient, you should delete this message. Any disclosure, copying, or distribution of this message, or the taking of any action based on it, is strictly prohibited.

Phishing


File "[redacted] Cash Position Report - Oct19 (1).xlsx" has been shared with you.

SO

SharePoint Online <no-reply@sharepointonline.com> [redacted]@[redacted].com>

Friday, October 18, 2019 at 2:54 AM

Show Details

[redacted] report attached. Refer to pivot tab

This link only works for the direct recipients of this message.

[redacted] Cash Position Report - Oct19 (1).xlsx

Open

Microsoft OneDrive

Sender will be notified when you open this link for the first time.

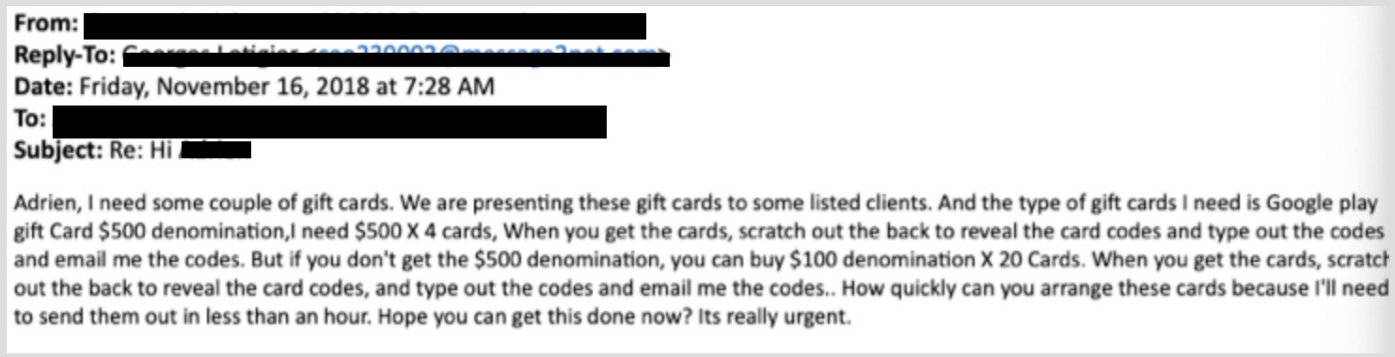
Microsoft respects your privacy. To learn more, please read our Privacy Statement.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

> **Phishing/social engineering accounted for 52% of cyberattacks against SMBs in 2018**
> *-Keeper/Ponemon*

SPEAR PHISHING EXAMPLES

There are no shortage of ways to trick people into giving up sensitive data and credentials. However, there are some well-honed attacks that spear phishers turn to time and again.

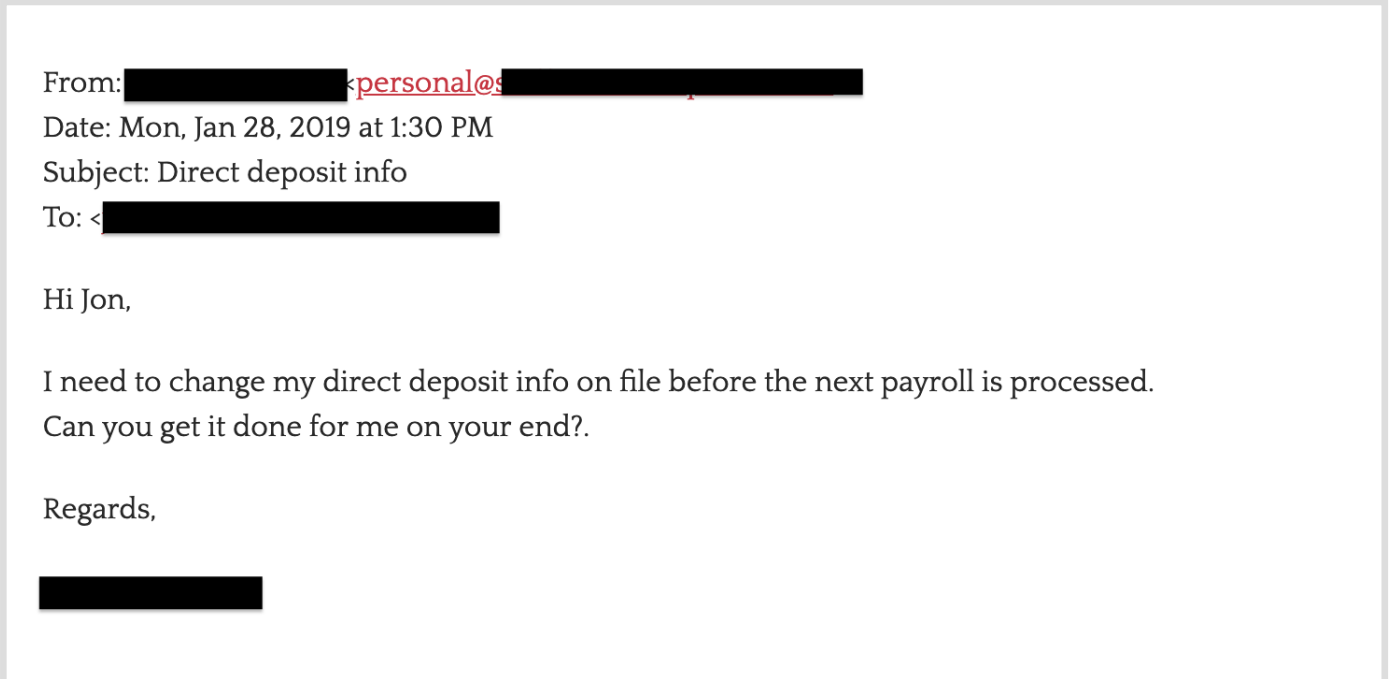
Gift Card Requests: Posing as an executive, a hacker asks an employee to purchase multiple gift cards and send them the codes on the back of the cards. Often, the hacker will say that they're in a meeting or away from their office. This adds to the believability of an executive writing an email from a personal email address, such as Gmail or Yahoo.



From: [redacted]
Reply-To: [redacted]
Date: Friday, November 16, 2018 at 7:28 AM
To: [redacted]
Subject: Re: Hi [redacted]

Adrien, I need some couple of gift cards. We are presenting these gift cards to some listed clients. And the type of gift cards I need is Google play gift Card $500 denomination,I need $500 X 4 cards, When you get the cards, scratch out the back to reveal the card codes and type out the codes and email me the codes. But if you don't get the $500 denomination, you can buy $100 denomination X 20 Cards. When you get the cards, scratch out the back to reveal the card codes, and type out the codes and email me the codes.. How quickly can you arrange these cards because I'll need to send them out in less than an hour. Hope you can get this done now? Its really urgent.

Direct Deposit Changes: In one version of this scam, a hacker posing as an employee sends an email to an HR assistant, requesting to change their bank account for their payroll direct deposit. In another version, a hacker posing as a vendor emails a staff member in accounting, informing them that the company's bank account and routing number has changed, and future payments should be sent to the new account.



From: [redacted] <personal@[redacted]
Date: Mon, Jan 28, 2019 at 1:30 PM
Subject: Direct deposit info
To: <[redacted]

Hi Jon,

I need to change my direct deposit info on file before the next payroll is processed.
Can you get it done for me on your end?.

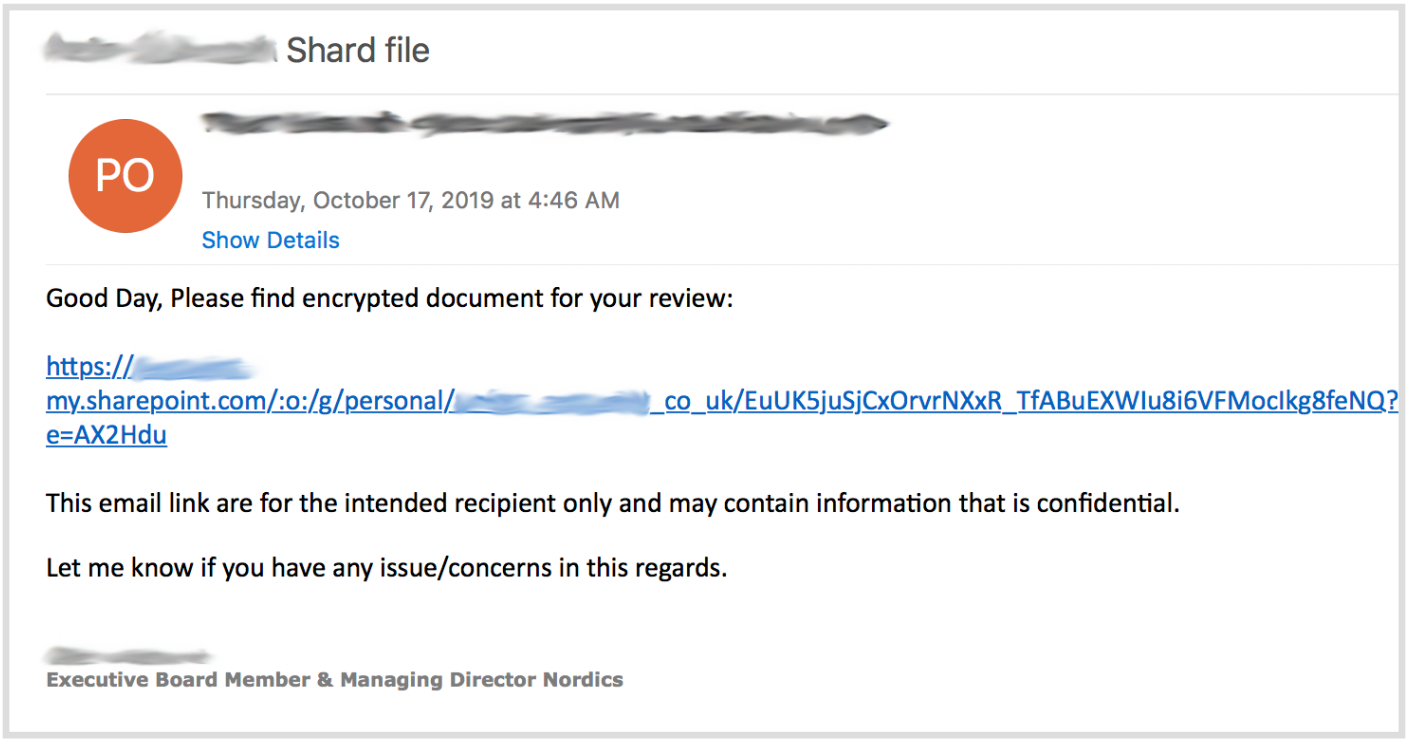
Regards,

[redacted]

W-2 Spear Phishing: A spear phisher posing as an executive emails a staff member in the HR department, requesting employee W-2s, a US tax form reflecting employee earnings and tax deductions. Tax time is particularly stressful for accounting and HR departments, and the pressure, in addition to the time constraints, makes them vulnerable to making the mistake of falling for this type of attack.

Wire Transfer Requests: Also known as business email compromise (BEC), this spear phishing variant is one of the most costly. A hacker posing as a top executive makes a request for funds in the form of a wire transfer. In many high-profile cases, businesses were completely unaware that millions of dollars had been sent to fraudulent bank accounts.

Multiphase Attacks: A common method for hacking into Microsoft 365, multiphase attacks begin with phishing and evolve into spear phishing. A hacker sends a phishing email to an employee, impersonating Microsoft. The victim unknowingly gives up their Microsoft 365 login credentials on a phishing page. Armed with the victim's username and password, the hacker enters the business's Microsoft 365 ecosystem where they launch spear phishing attacks using legitimate Microsoft 365 email addresses.


[redacted] Shard file

PO

[redacted]

Thursday, October 17, 2019 at 4:46 AM

Show Details

Good Day, Please find encrypted document for your review:

https://[redacted]
my.sharepoint.com/:o:/g/personal/[redacted]_co_uk/EuUK5juSjCxOrvrNXxR_TfABuEXWIu8i6VFMoclkg8feNQ?e=AX2Hdu

This email link are for the intended recipient only and may contain information that is confidential.

Let me know if you have any issue/concerns in this regards.

[redacted]

Executive Board Member & Managing Director Nordics

> **There were more than 20,000 US victims of business email compromise in 2018**
> *- FBI*

SPEAR PHISHING TECHNIQUES

A one-off, text-only spear phishing email might look unsophisticated on the surface, but there are social engineering techniques at work that reveal a sophisticated level of psychological manipulation. Below are some examples:

Engaging in pretexting: Spear phishers prime their victims by first sending a friendly email and engaging in small talk, such as "how was your vacation?" or "congrats on the promotion." This lowers the victim's guard, prepping them for the spear phisher's eventual request, which might not come for several more emails.

Sent: Monday, February 25, 2019 at 11:52 AM
From: "[redacted]
To: "[redacted]
Subject: RE: DD

Hi [redacted]

I enjoyed our visit in Atlanta. I am planning on working from Denver the week of March 11th.

Please login to www.myadp.com and update your direct deposit info. Payroll has been processed for 2/28.

Thank you,
[redacted]

Making urgent requests: Often, spear phishers will convince their victims that they have only hours—or even minutes—to send a wire transfer, change their bank account information, or purchase gift cards for clients.

Sending emails via mobile: Spear phishers posing as executives often claim to be out of the office, even out of the country, and urgently need the victim's help. Adding "sent from my iPad, iPhone, or Android device" adds to the believability of such a claim and also excuses mistakes in the email, such as typos. It also creates an excuse for using a non-corporate email address like Gmail.

[redacted]

GL [redacted] <president.[redacted].com>
To: [redacted]
Monday, May 6, 2019 at 12:35 PM
Hide Details

I have important request i need you to handle immediately. Kindly confirm your availability.

Regards.

Sent from my Verizon 4G LTE Droid - please excuse any brevity or typos

SPEAR PHISHING PREVENTION

The absence of URLs and attachments makes spear phishing extremely difficult to detect. Traditional email filters use outdated methods to block threats, and most are ineffective in the fight against spear phishing. Optimal spear phishing protection requires advanced methods.

TRADITIONAL EMAIL DEFENSE

Reputation: Reputation-based threat detection blocks known, malicious email senders (IP addresses) and phishing URLs. A reputation-based filter will block bad senders known to the filter but will miss new threats.

Signature (Fingerprint): Signature-based threat detection blocks threats with a known "signature," such as malware code.

Sandboxing: Sandboxing sends suspicious emails to a controlled environment for analysis. It's ineffective against spear phishing emails that do not include attachments or links.

Secure Email Gateways: Secure email gateways (SEG) rely on reputation and signature-based detection. A SEG sits outside of Microsoft 365 architecture, disabling Exchange Online Protection (EOP) and leaving Microsoft 365 unprotected against insider attacks.

> **Native Office Microsoft email security has a total accuracy rating of only 8%**
> *- SE Labs*

PREDICTIVE DEFENSE

With predictive defense, artificial intelligence (AI), including a combination of supervised and unsupervised machine learning models, work together to identify the telltale and difficult-to-detect signs of spear phishing:

Supervised Learning: Algorithms are trained with malicious and legitimate and emails to recognize specific features of spear phishing emails, such as mobile signatures and email addresses from public domains.

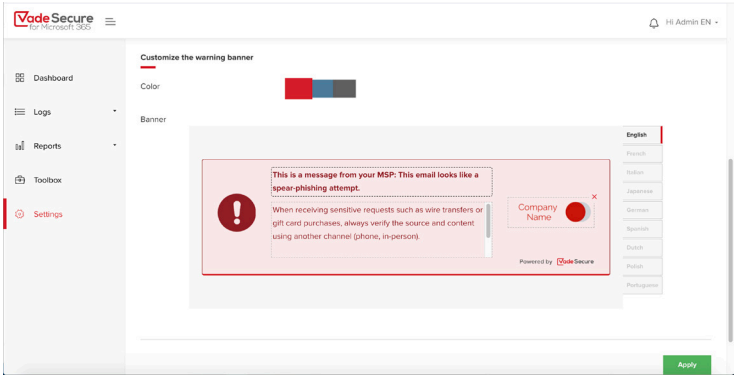
Unsupervised Learning: Natural Language Processing and Unsupervised Anomaly Detection recognize abusive patterns in spear phishing emails, including urgency, flag words, and email addresses that do not match senders in a business's entity model.

User Feedback Loops: Users report spear phishing emails to the security operations team (SOC), which analyzes the email and improves the algorithms.

Vade Secure for Microsoft 365

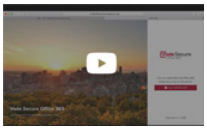
Our AI-based anti-spear phishing technology features customizable warning banners to alert Microsoft 365 users of suspected spoofing attempts.

Ask for a Demo



SPEAR PHISHING RESOURCES

Data Sheet:
Why Partner With Vade Secure?



Video:
Spear Phishing Detection with Vade Secure for Microsoft 365

Data Sheet:
Vade Secure for Microsoft 365

Data Sheet:
Anti-Spear Phishing