INKY™

Welcome to 2019: Phishing Gets Personal

Email Security Report

The holiday period is typically the peak time of year for online shopping, and with that comes higher rates of cybercrime, especially phishing scams. Fourth quarter of 2018 was no different. At INKY, 2018 was a year of unprecedented growth both in terms of our customer base and the millions of emails we processed through our email security platform. The more emails we process, the more phish we catch. Of all the phishing attempts that came up against our platform in 2018, we saw zero successful attacks.

While none of the attacks made it through, we decided to analyze a subset of the messages that INKY flagged as high confidence phishing predictions. The following analysis speaks to the robustness of our platform and critically underlines the unfortunate persistence of phishing attacks and their increasing sophistication.

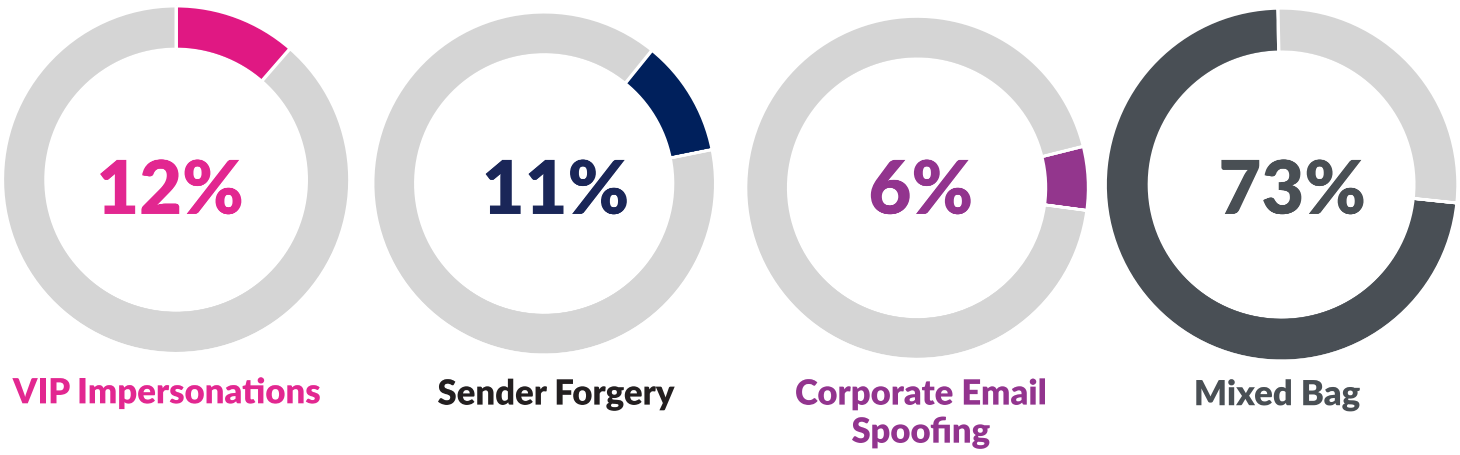
INKY®

Email Security 4Q18 Analysis

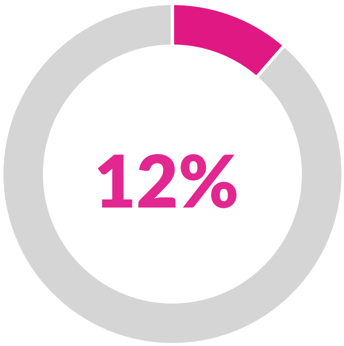
4Q18 was a busy period for phishing scammers. INKY researchers saw a spike in email volume this time of year as people use email to gather their receipts from online shopping, shipping notifications, returns, and virtual holiday greetings. We analyzed the highest volume attack types and broke down each one. The majority of attacks we analyzed showed an increase in target personalization, making them considerably more difficult to detect by the human eye.

KEY FINDINGS

- **12% of phishing attacks took the form of VIP Impersonations**
- **11% assessed phishing attacks were Sender Forgery**
- **6% Corporate Email Spoofing**



Corporate VIP Impersonation



VIP Impersonations

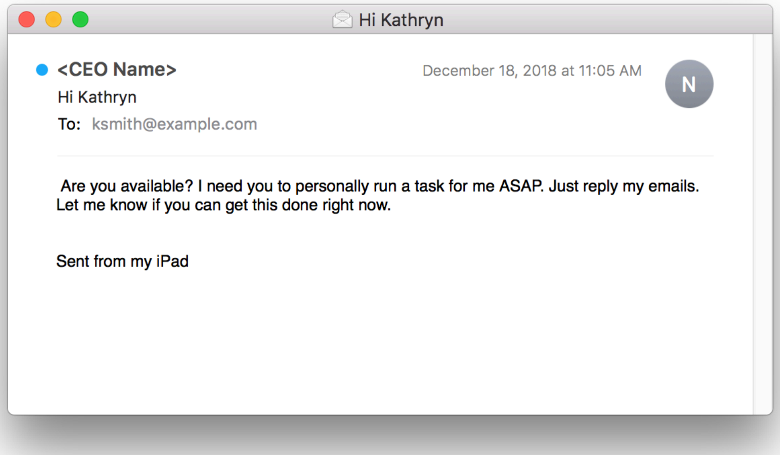
The 4th quarter of 2018 was a particularly robust period for VIP impersonations. This type of attack is usually fairly involved and often delivered in real-time. A typical scheme can involve a scenario where the CEO (or perhaps someone from finance) is in a meeting or limited cellphone reception area where a confirmation call is not possible. The victim then becomes engaged with a request for help which eventually leads to handing over sensitive data without verification to the scammer on the other end.

Of the sample group, 12% came under this category. Commonalities include:

- The name of a CEO or Finance professional is usually attached to the email; these names are easily sourced from social media sites or corporate filings.
- While the name will be familiar to the victim, they most often come from an unauthorized email address that in some cases represent as plausible personal email for the sender.
- The mail may have a header like “From: Mark Zuckerberg <ceo@execmail.net>”
- The actual email addresses frequently have terms like “CEO” or “exec” to sound more official. Making these more difficult to detect, many mail clients (particularly mobile ones) prefer to show only the display name and make it hard to see the sender’s email address.
- In some of the examples we examined the VIP no longer works for the company, suggesting that the scammers are mining public data sources like LinkedIn, news articles, or the company’s own About/Leadership web pages.
- Most of the requests attempt to create a false sense of urgency, requesting that the recipient perform a task but say the recipient should only communicate via email.
- Many of the requests have a signature that suggests they’ve been sent from a mobile device, like a tablet. This technique is to support the impression that they are unreachable by phone.

Corporate VIP Impersonation

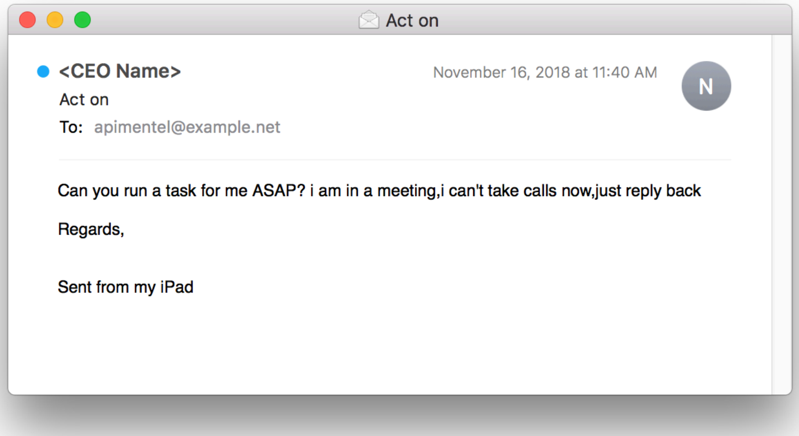
This type of attack is unfortunately not going anywhere. We predict that they will only increase. The virtualization of corporations and the dispersal of staff is a modern reality, and while there are some companies whose products necessitate brick and mortar facilities, more and more workers are taking up remote assignments, and colleagues are becoming more commonly defined by their digital presence. The digital associate is the prime candidate for a VIP attack.



<CEO Name> December 18, 2018 at 11:05 AM
Hi Kathryn
To: ksmith@example.com

Are you available? I need you to personally run a task for me ASAP. Just reply my emails. Let me know if you can get this done right now.

Sent from my iPad

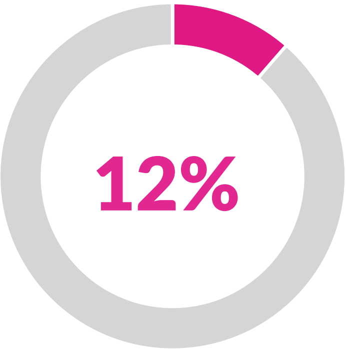


<CEO Name> November 16, 2018 at 11:40 AM
Act on
To: apimentel@example.net

Can you run a task for me ASAP? i am in a meeting,i can't take calls now,just reply back

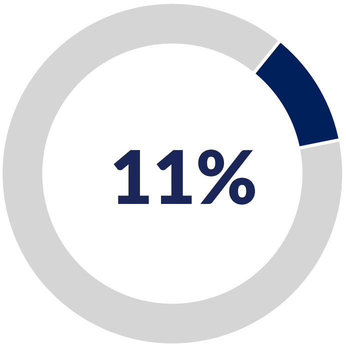
Regards,

Sent from my iPad



of phishing attacks took the form of VIP Impersonations

Sender Forgery



Sender Forgery

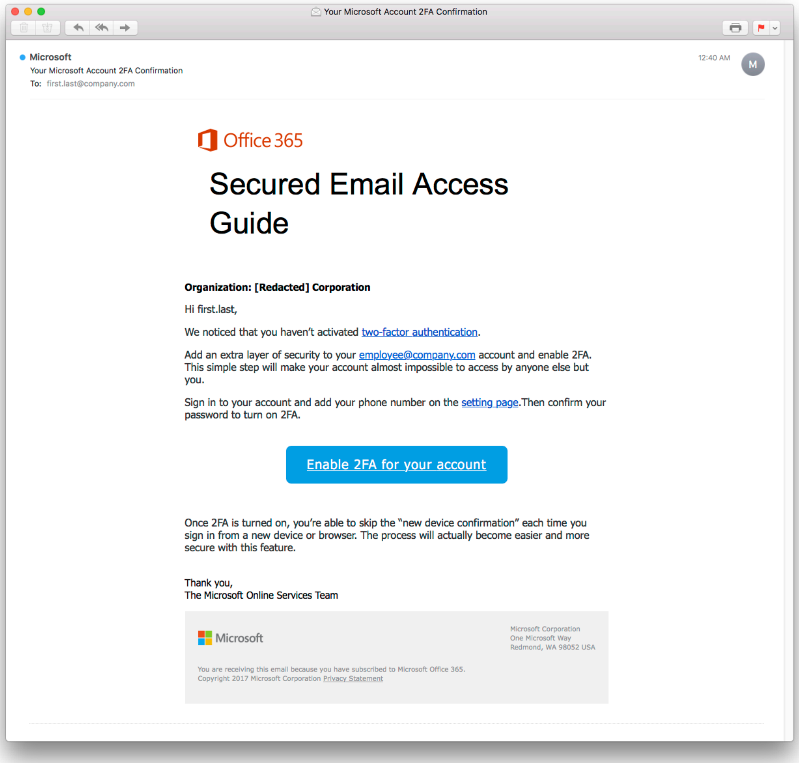
An email that presents itself as having come from a known contact is a classic in terms of phishing attacks. This type of attack perseveres as contacts maintain personal and professional emails. Often contacts cycle through Gmail, Yahoo and other popular mail providers, making it difficult to discern a legitimate message from a phishing attack.

In our sample, a full 11% were found to be in the Sender Forgery category. We've summarized their commonalities as follows:

- Spoofing a name of a known contact is common, and exceedingly easy. Any kind of publicly shared social media account allows even an amateur phisher to establish a lengthy list of a victim's known contacts.
- Corporate email addresses are easy to find and spoof. Once a phisher establishes the format of a corporate email, spoofing the sender can be easily accomplished.
- In many of the examples, the mail says it's from a contact "John Smith" but the mail is significantly different than their normal mail (different mail client, country of mail servers as an example).

Sender Forgery Examples

While email users are becoming more sophisticated in their ability to discern obvious phishing attacks, like the Nigerian Prince as a classic example, emails that come from a familiar name continue to be successful. Phishing victims are far more likely to open an email that profess a call to action from a purported friend or known contact than they are from a sender they don't recognize.



Your Microsoft Account 2FA Confirmation

Microsoft
Your Microsoft Account 2FA Confirmation
To: first.last@company.com

12:40 AM

Office 365

Secured Email Access Guide

Organization: [Redacted] Corporation

Hi first.last,

We noticed that you haven't activated two-factor authentication.

Add an extra layer of security to your employee@company.com account and enable 2FA. This simple step will make your account almost impossible to access by anyone else but you.

Sign in to your account and add your phone number on the setting page.Then confirm your password to turn on 2FA.

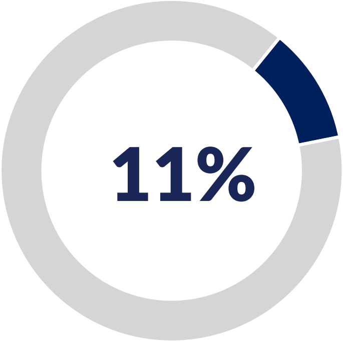
Once 2FA is turned on, you're able to skip the "new device confirmation" each time you sign in from a new device or browser. The process will actually become easier and more secure with this feature.

Thank you,
The Microsoft Online Services Team

Microsoft

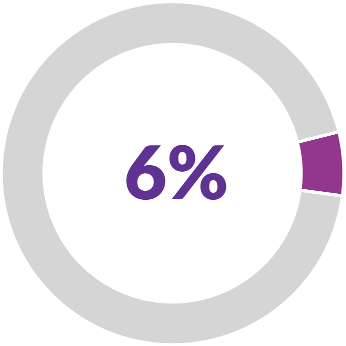
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052 USA

You are receiving this email because you have subscribed to Microsoft Office 365.
Copyright 2017 Microsoft Corporation Privacy Statement



of phishing attempts were in the form of Sender Forgery

Corporate Email Spoofing



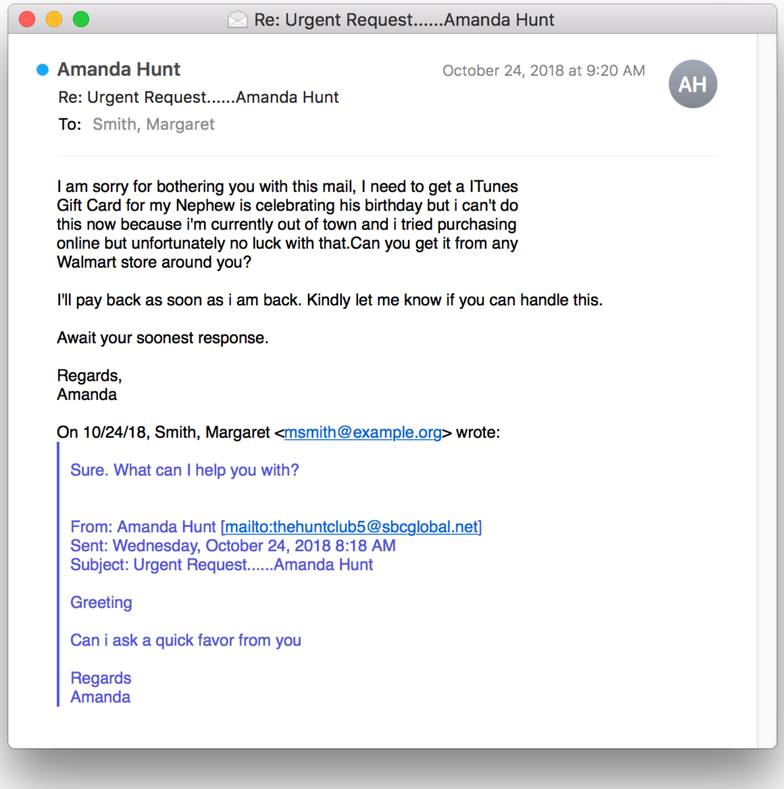
Corporate Email Spoofing

Corporate email spoofing blends the elements of VIP impersonation with sender forgery. This type of attack is sophisticated in that it deliberately targets a specific corporate entity. This type of attack often occurs after a major announcement. The nature of the announcement has no bearing on the frequency of the attacks, both positive and negative news can be leveraged to provide cover for the phishing attacker's true intentions. In the past (and for those remaining unprotected) corporate spoofing has resulted in the loss of corporate intellectual property, private information, financials and even protected healthcare information.

This category makes up 6% of the total of that we caught. Here are the key elements of this type of attack:

- The sender spoofs a corporate email address figuring out if a corporation is FLast, first.last or last.first.
- For example, the mail has a forged header like "From: mailbox@company.com" but it really came from outside the company.com mail server.
- This type of attack is often designed to extract key corporate information or to prompt a malware or spyware download onto corporate assets

Corporate Email Spoofing Example



Amanda Hunt
October 24, 2018 at 9:20 AM
Re: Urgent Request......Amanda Hunt
To: Smith, Margaret

I am sorry for bothering you with this mail, I need to get a ITunes Gift Card for my Nephew is celebrating his birthday but i can't do this now because i'm currently out of town and i tried purchasing online but unfortunately no luck with that.Can you get it from any Walmart store around you?

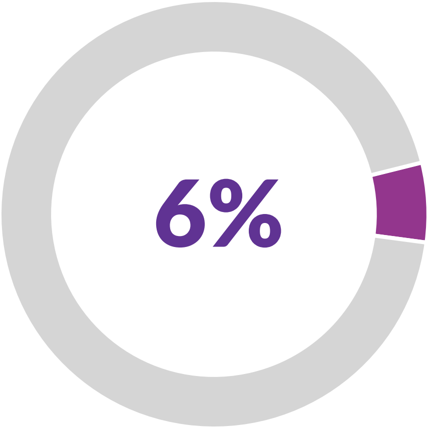
I'll pay back as soon as i am back. Kindly let me know if you can handle this.

Await your soonest response.

Regards,
Amanda

On 10/24/18, Smith, Margaret <msmith@example.org> wrote:

> Sure. What can I help you with?
>
> From: Amanda Hunt [mailto:thehuntclub5@sbcglobal.net]
> Sent: Wednesday, October 24, 2018 8:18 AM
> Subject: Urgent Request......Amanda Hunt
>
> Greeting
>
> Can i ask a quick favor from you
>
> Regards
> Amanda

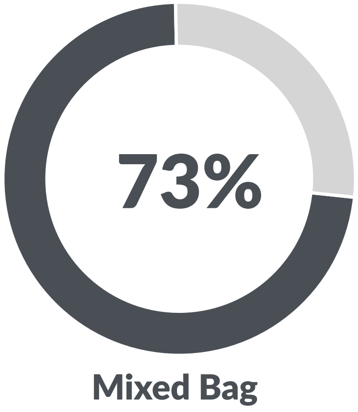


of phishing attempts were Corporate Email Spoofing as seen above

Of the emails analyzed in Q4, INKY found that publicly traded companies and private companies suffer this kind of attack on a fairly equal basis. Public companies have an obligation to release earnings announcements and private companies often announcing venture capital, acquisitions or other investments, providing phishing scammers with plenty of reasons to spool up forged corporate email addresses and attempt to exploit the corporation's associates.

The Best of the Rest

The remaining 73% of the phishing attempts we analyzed are a mixed bag of awful. Most are personalized to the recipient's company name or the recipient's own personal information based on exploiting data breaches. Q4 2018 was particularly nasty as the holiday season was ruthlessly and relentlessly exploited by phishing scammers.

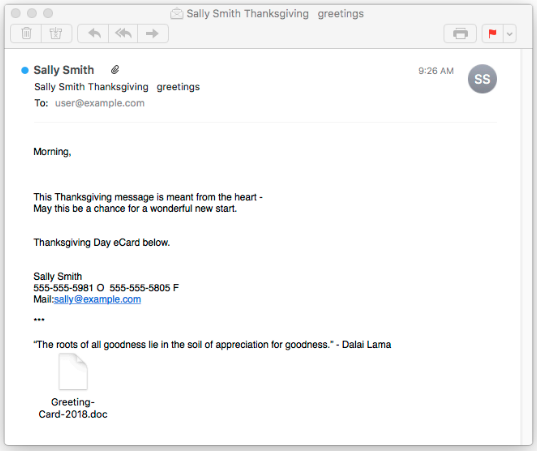


Here is a summary of some of the phish INKY caught in her net:

- Fake IT help desk / Mail server alert messages about expired passwords, failed syncing, undelivered messages, etc. These typically try to get the user to click a call-to-action link to "recover messages" or "update now," but the links go to fake login pages to harvest account credentials. These very often have the target company name somewhere in them, to make it seem like they're internal messages. For example, "From: Acme Corp IT Desk, Subject: Mail server update".
- Fake voicemail or fax notifications with malicious attachments or links to malicious downloads. These will say the recipient (identified by name or email) received a voicemail and offer a file or link to retrieve it.
- Fake invoice notifications with malicious attachments. These often come from compromised accounts of business partners so they seem especially real.
- Bitcoin blackmail scams that claim to have an old password and threaten to release compromising information if the recipient doesn't send them ransom via Bitcoin. The passwords mentioned are real and known based on data breaches.
- Thanksgiving / Seasons Greetings cards from the boss that contain some poetic holiday message and a malicious download posing as a Word file like Greeting_Card_2018.doc. These have the real CEO's name in the headers, subject, or message like "From: mark@facebook.com, Subject: Mark Zuckerberg Happy Holidays".
- Delivery notification/updates were particularly prevalent during 4th quarter the majority of these mimicked FedEx, UPS or USPS iconography, contained legitimate links to the respective organizations but provided a tracking number that acted as a nefarious call to action.

Other Phishing Email Examples

Of course, there are other brand impersonations with supposed holiday sales or bank account updates, but we saw much more clever and personalized phishing emails like these in this last quarter.


Sally Smith Thanksgiving greetings

Sally Smith
Sally Smith Thanksgiving greetings
To: user@example.com

9:26 AM

Morning,

This Thanksgiving message is meant from the heart -
May this be a chance for a wonderful new start.

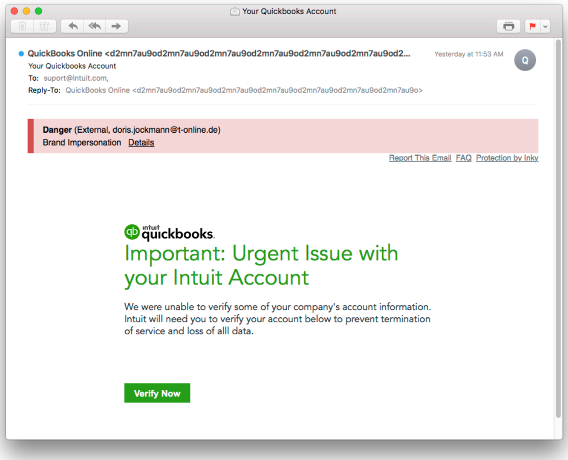
Thanksgiving Day eCard below.

Sally Smith
555-555-5981 O 555-555-5805 F
Mail:sally@example.com

•••

"The roots of all goodness lie in the soil of appreciation for goodness." - Dalai Lama

Greeting-Card-2018.doc


Your Quickbooks Account

QuickBooks Online <d2mn7au9od2mn7au9od2mn7au9od2mn7au9od2mn7au9od2mn7au9od2...
Your Quickbooks Account
To: suport@Intuit.com,
Reply-To: QuickBooks Online <d2mn7au9od2mn7au9od2mn7au9od2mn7au9od2mn7au9od2mn7au9od2mn7au9o>

Yesterday at 11:53 AM

Danger (External, doris.jockmann@t-online.de)
Brand Impersonation Details

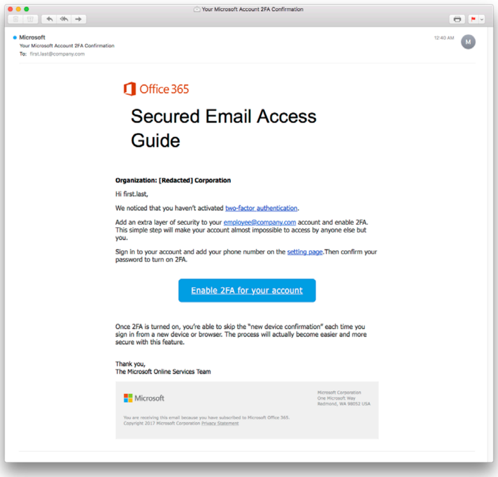
Report This Email FAQ Protection by Inky

intuit quickbooks

Important: Urgent Issue with your Intuit Account

We were unable to verify some of your company's account information. Intuit will need you to verify your account below to prevent termination of service and loss of alll data.

Verify Now


Your Microsoft Account 2FA Confirmation

Microsoft
Your Microsoft Account 2FA Confirmation
To: first.last@company.com

12:40 AM

Office 365

Secured Email Access Guide

Organization: [Redacted] Corporation

Hi first.last,

We noticed that you haven't activated two-factor authentication.

Add an extra layer of security to your employee@company.com account and enable 2FA. This simple step will make your account almost impossible to access by anyone else but you.

Sign in to your account and add your phone number on the setting page.Then confirm your password to turn on 2FA.

Enable 2FA for your account

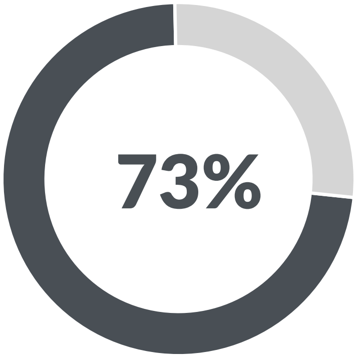
Once 2FA is turned on, you're able to skip the "new device confirmation" each time you sign in from a new device or browser. The process will actually become easier and more secure with this feature.

Thank you,
The Microsoft Online Services Team

Microsoft

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052 USA

You are receiving this email because you have subscribed to Microsoft Office 365.
Copyright 2017 Microsoft Corporation Privacy Statement



Mixed Bag

Conclusions

92% of Malware is delivered by email. The cost of successfully executed Q4 phishing attacks will be in the billions of dollars. At INKY we find this to be unacceptable and unnecessary.

The reality is that older generation phish filters are simply not capable of identifying the personalized attacks that were so prevalent in Q4. The statistical Bayesian-based methods that traditional phish filters employ are effective at identifying mass trawling efforts but fail badly when the attack is targeted. Training programs build awareness but their failure in Q4 as it was for all of 2018 will again be measured in the billions. The time for relying on associates as a competent, qualified and aware cyber defense has passed. Educated associates are vital, but their effectivity as a deterrent is daily undermined.

At INKY we believe in email and are dedicated to ensuring its fidelity. INKY is not a platform with equals. It's a generation ahead of anything else out there and until the use of technologies like ours becomes more prevalent, the financial and human carnage caused by phishing will only continue.

https://www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html