

Email, the easiest way to breach your security

Jake Ruddy



Email

A BRIEF HISTORY



Email didn't start as email

- Email is technically older than ARPANet or the Internet
- In the beginning users left messages in a file directory
- In 1965 a system called MAILBOX was used at MIT. This system allowed users to communicate on the same computer. Users used “dumb terminals” to access a mainframe and could communicate with each other.
- Roy Tomlinson is credited with inventing email in 1972
- By 1974 there were hundreds of military email users
- Within a couple of years 75% of all ARPANet traffic was email
- Eventually “offline readers” were created, think Outlook, AOL, Eudora, Thunderbird, Pegasus
- Finally web based readers emerged, think Yahoo and Hotmail

Email

STATISTICS



Massive Adoption – 2017 Stats

- Each day, the average worker receives 121 emails and sends 40.
- 86% of professionals name email as their favorite communication tool.
- 66% of email is read on mobile devices.
- 49.7% of email is considered spam.
- 2.3% of emails have a malicious attachment
- The top day for email is Cyber Monday
- 33% of mobile users say they've read an email based on its subject line.
- More emails are opened on Tuesday than any other day of the week.

Email

BY THE NUMBERS



What Happens in a Day?

- Roughly 269 billion emails were sent per day worldwide in 2017.
- In 2022, it is expected to increase to over 333 billion emails per day.

WHAT ARE THE THREATS?

Malware

Malware

WHAT EXACTLY IS IT?

Malware is short for “malicious software”

This general term covers all types of computer programs that are designed to damage a computer, server, or network.

This also includes mobile devices.

1

Malware threats are further defined by the way they spread and what they do.

2

In December 2017 McAfee Labs published their annual Threat Report.

The McAfee Labs counted an all-time high of 57.6 million new samples in Q3 alone.

3

Malware continues to grow at a rapid pace in 2018 with crypto mining leading the pack currently.

WHAT ARE THE THREATS?

Viruses

Viruses

COMPUTER CAUGHT A COLD

A computer virus is designed to spread from host to host and can replicate itself.

They often attach themselves to a legitimate program or file. Once executed it will follow a specific set of instructions.

Viruses require a user to trigger the program or boot from an infected disk or USB device.

1

Self-replicating programs were first established in 1949.

2

Frederick Cohen coined the term "Virus" for computer programs that were infectious due to their tendency to replicate in 1983.

3

Symantec launched one of the first antivirus programs called Norton Antivirus in 1990.

WHAT ARE THE THREATS?

Worms

Worms

AN ADVANCED COLD

A computer worm is similar to a virus but does not require user action to spread.

After a worm is activated it copies itself to another computer and then launches that copy. They can spread across networks very rapidly.

1

In 1988 The Morris Worm was designed as a test and it slowed down the internet due to spreading so quickly.

2

MyDoom was created in 2004 and was labeled the fastest mailer worm and allowed hackers access to infected computers.

3

The recent NSA-derived WannaCry ransomware worm shut down over 75,000 computers and affected at least 74 countries.

WHAT ARE THE THREATS?

Trojans

Trojans

A HIDDEN THREAT

A Trojan is malware that is hidden inside of programs.

Trojans are often hidden inside of legitimate software that have been compromised and redistributed.

Mobile apps often pose as legitimate programs but contain Trojans.

1

Trojans often contain a downloader that downloads and installed additional pieces of malware.

2

Trojans often delete, copy, or modify data.

3

Trojans are a very popular tool used to steal credentials, deploy ransomware, and create back doors on networks.

WHAT ARE THE THREATS?

Ransomware

Ransomware

SHOW ME THE MONEY

Ransomware is malware that blocks system access until a sum of money is paid.

This form of malware has generated tens of millions of dollars to date.

It uses encryption to hold files ransom. Files cannot be restored without the keys for decryption or doing a full restore from backup.

1

Antivirus will not prevent a ransomware infection.

2

Ransomware is often deployed remotely, using an infected system. It can also be triggered by clicking a link in an email or attachment.

3

Ransomware can also be deployed via a Trojan.

WHAT ARE THE THREATS?

Cryptojacking

Cryptojacking

LET ME BORROW YOUR CPU

The unauthorized use of someone's computer to mine cryptocurrency.

This is currently the number one favorite amongst cyberthieves.

This threat not only attacks enterprise networks but also goes after websites and data centers.

1

Fairly easy to detect on most business networks using antivirus and antimalware scans.

2

Difficult to track on websites because attackers are usually compromising code running on servers and not in the operating system itself.

3

There are some legitimate uses and some users allow this on their computer in order to collect money.

WHAT ARE THE THREATS?

Phishing, Spear Phishing, and Whaling

Phish·ing

/ˈfɪʃɪŋ/



Most often spread via mass emails

- Phishing is an attempt to gain access to sensitive information such as usernames, passwords, and credit card details.
- Email spoofing is the most common delivery method. Emails purporting to be from your bank, PayPal, cloud services, social media websites, or IT administrators encourage you to click links that redirect you to a compromised site.

Spear Phishing

/ˈfiʃɪŋ/



Directed at specific individuals or companies

- Focused attempts of phishing where the attacker has often does research to increase the probability of success.
- Emails are spoofed from clients and potential vendors. Sometimes come directly from a compromised client email account.

Whal·ing

/'(h)waliNG/



Spear phishing attacks that are specifically directed at senior executives and other high-profile targets

- Focused attempts of phishing where the attacker has often does research to increase the probability of success.
- Emails are spoofed from clients and potential vendors. These may be sent as complaints, subpoenas, or another executive level issue.

WHAT ARE THE THREATS?

Examples

From: Microsoft Outlook. [mailto:admin@jpfincialagency.com]

Sent: Tuesday, March 07, 2017 11:48 AM

To:

[http://www.realestatemenu.ca/ Step Validation Process\)](http://www.realestatemenu.ca/Step Validation Process)

<wp-admin/footmat.htm>

Click to follow link



Dear User,,

Your Microsoft Outlook Account Requires an Urgent Validation to ensure it would not be deactivated within 24 hours.

Proceed to Microsoft Outlook Validation page by clicking on the icon below to get started

[Get Started](#)

Thank you for using Microsoft Outlook.

To stop separating items that are identified as clutter, go to Options. To stop receiving notifications about Clutter, go to Options and turn them off. This system notification isn't an email message and you can't reply to it.

"
-





Send	To...	
	Cc...	
	Subject	FW: GoDaddy --User Verification

From: GoDaddy <security-alert@godaddy.com> [<mailto:parsadc@mymts.net>]
Sent: Saturday, March 04, 2017 9:16 AM
Subject: GoDaddy --User Verification

Dear GoDaddy Client,

Your access has been locked out for verification

Your safety is our top priority click below to restore access

[http://validste.goodaddy.com.
infocreatives.com/v2/sec/index.php](http://validste.goodaddy.com.infocreatives.com/v2/sec/index.php)
Ctrl+Click to follow link

<https://support.godaddy.com/Login.aspx>

Thank you.

© Copyright 2017 GoDaddy. All rights reserved.

FILE MESSAGE

Ignore Delete Reply Reply All Forward Meeting Dell Orders To Manager Rules OneNote Mark Categorize Follow Translate Find Find Related Select Zoom

Junk Delete Reply Reply All Forward Meeting Dell Orders To Manager Rules OneNote Mark Categorize Follow Translate Find Find Related Select Zoom

Quick Steps Move Tags Editing Zoom



Thu 3/30/2017 11:50 AM

FW: Your Order Information 746282284

To Jake Ruddy

Cc

You replied to this message on 3/30/2017 11:51 AM.

On Mar 29, 2017, at 7:14 PM, MEMORY4LESS.COM Support <gnaabn@zorzodesign.com> wrote:

Hello,
Check your order.



Invoice #: 746280832
Created: March 28, 2017
Due: March 31, 2017

MEMORY4LESS.COM

1504 W. Commonwealth Ave, Suite B
Fullerton, CA 92833

Payment Method

Credit Card 1

Item Price

Sun 2GB PC2-5300 DDR2-667MHz ECC Registered CL5 240-Pin DIMM Dual Rank Memory Module Mfr P/N 371-4158-N \$275.00

Shipping (Overnight Delivery) \$16.99

<https://docs.google.com/uc?authuser=0&id=0bwhynpfwly6begdybw9xc3qxtgs&export=download>
Click to follow link

[Get Full Order Information](#)

To get more information about your order and tracking number, check your full order!





Verify a recent charge attempt



Dear Membership

Account :
37***



Fraud Protection

[View Now](#)

For your security, we regularly monitor accounts for possible fraudulent <https://t.co/kKSYdrXix>

Below are the details of an attempted charge:

Payment Due Date:	October 11, 2018
Merchant information:	walmart.com
Amount:	\$890.00
Status:	Not Approved

For your security, new charges on the accounts listed above may be declined. If applicable, you should advise any Additional Card Member(s) on your account that their new charges may also be declined. To safeguard your account, please access your account [Visit Here](#).

Thank you for your Card Membership.

American Express Customer Care



START A NEW DISCUSSION

Join Community @Amex



[Like Us](#) on Facebook



[Follow Us](#) on Twitter



[Subscribe](#) to our channel



[Share](#) with Foursquare friends

[Contact Us](#)

[Privacy Statement](#)

[Add us to your address book](#)

Your Card Member information is included above to help you recognize this as a customer service e-mail from American Express. To learn more about e-mail security or report a suspicious e-mail, please visit us at americanexpress.com/phishing. We kindly ask you not to reply to this e-mail but instead contact us via [customer service](#).

© 2018 American Express. All rights reserved.

AGNEUBBK0002003



Doc 12-19-16.pdf - Adobe Acrobat

File Edit View Window Help

Open Create

1 / 1 100%

Tools Fill & Sign Comment



Adobe® Creative Cloud™

[View pdf File](#)



<http://www.magtechprints.pl/modules/wp-mail1.php>

The image shows a screenshot of the Adobe Acrobat application window. The window title is "Doc 12-19-16.pdf - Adobe Acrobat". The menu bar includes "File", "Edit", "View", "Window", and "Help". The toolbar contains various icons for file operations like "Open" and "Create", as well as navigation and tool icons. The main content area displays the Adobe Creative Cloud logo and the text "Adobe® Creative Cloud™". Below this, there is a red button labeled "View pdf File" and a yellow circular icon with a padlock and the text "100% SECURE". A URL is displayed below the button: "http://www.magtechprints.pl/modules/wp-mail1.php". The window also shows a sidebar on the left with icons for document navigation and a status bar at the bottom with "1 / 1" and "100%".



RE: Undelivered Mails: Your account has 84 pending inbox mails

File Message Tell me what you want to do...

Ignore Delete Reply Reply All Forward More Meeting To Manager Done Create New Rules OneNote Actions

Jake Ruddy

RE: Undelivered Mails: Your account has 84 pending inbox mails

To: PCS Support Staff <help@helpmepcs.com>
Subject: FW: Undelivered Mails: Your account has 84 pending inbox mails

This seems like spam to me.

From: OutlookOffice365 <admin@burymodelfc.co.uk>
Sent: Tuesday, September 18, 2018 9:35 AM
To: Barb <>
Subject: Undelivered Mails: Your account has 84 pending inbox mails

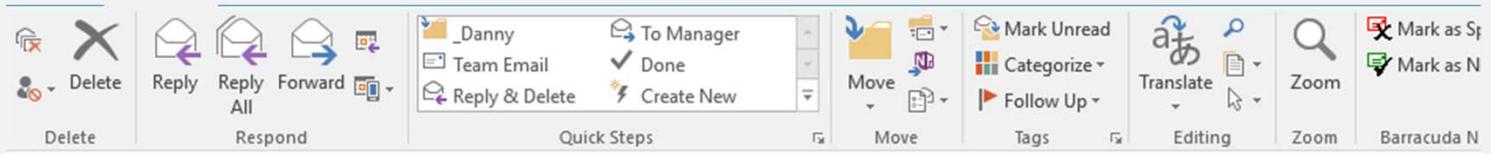
Error Pending Messages Action Required

Hi

You have received 84 pending messages from <http://www.cultivoselamanecer.com.ar/> on September 17th, 2018 1:00 AM (UTC) which are listed below. Please take the appropriate action:

Click or tap to follow link.

[Click Here: Deliver Mails To Inbox](#)
[Click Here: Delete Mails As Spam](#)



Jake Ruddy | Dan
RE: You received notification from DocuSign Electronic Service

From: DocuSign Signature and Invoice [mailto:docusign@vsimportservices.com]
Sent: Wednesday, August 22, 2018 10:46 AM
To: , Dan <>
Subject: You received notification from DocuSign Electronic Service



Please review and sign an invoice.

<http://yapd.org?6q4zg=dbqhalyo1aysqr3luw>
Click or tap to follow link.

SEE DOCUMENT

Dear Receiver,

Please review this invoice
This is an electronically generated invoice notification.



From: Office Email Center [mailto:no-reply@autostorages.com]

Sent: Tuesday, June 12, 2018 1:28 PM

To:

Subject: Your Office Mail is Almost Full

Microsoft Email Office 365

Your Office MailBox is Almost Full

Total Storage [5000 MB] Used - 4964 MB.

Increase your storage below for free to enable your mailbox for more incoming messages and outgoing messages. If you take no action your inbox will stop working and you will not be able to receive incoming emails and sending emails.

Follow the free Storage with o

<https://ex-elec.co.uk/c562@/?email=susan@com>

Click or tap to follow link.

Free Storage With Office365

**Failure to Add more storage your
their will be stoppage of incoming email and outgoing emails.**

This message was sent from an Un-monitored e-mail address.

Please do not reply to this message.

Privacy | Legal Notices

Sincerely,

Microsoft Secure Department

© 2018 Microsoft Corporation. All Rights Reserved



A screenshot of a Windows desktop environment. The background is a red and pink abstract image. In the foreground, a Microsoft website is open in a Microsoft Edge browser window. The website has a blue header with the Microsoft logo and navigation links. The main content area features a large blue banner with the text "Call for support: +1-844-699-8351". Below the banner are several product tiles for Windows, Windows Phone 8, Lumia devices, Xbox, Office, and OneDrive. At the bottom, there are more product tiles for Surface, Microsoft Edge, Internet Explorer, Skype, Outlook.com, and MSN. Two security warnings are overlaid on the browser window. The first is a "Warning!" dialog box with the text: "** YOUR COMPUTER HAS BEEN BLOCKED ** Your computer has alerted us that it has been infected with a virus and spyware. The following information is being stolen... > Facebook Login > Credit Card Details > Email Account Login". The second is a "Windows Security" dialog box titled "Microsoft Edge" with the text: "The server shop-itwth-us.website is asking for your user name and password. The server reports that it is from 0x80070424 Microsoft Security Alert: Ransomware Threat Detected !!! Call Microsoft Help Desk: +1-844-699-8351 (TOLL-FREE) . Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure." Below this text are input fields for "User name" and "Password", and "OK" and "Cancel" buttons. The desktop taskbar on the left shows various application icons, including Recycle Bin, Microsoft Office Support, Google Chrome, and several PDF files. The taskbar at the bottom shows the Start button and several pinned application icons.

support.microsoft.com savs:



Call for support:
(877) 409-3489

Manage my account

Windows Security

The server gizanine.stream is asking for your user name and password. The server reports that it is from This URL has been blocked under instructions of a competent US Government Authority or in compliance with the orders of a Court of competent jurisdiction. Infringing or abetting infringement of copyright-protected content including under this URL is an offence in law. Ss. 63, 63-A, 65 and 65-A of the Copyright Act, 1957, read with Section 51, prescribe penalties of a prison term of upto 3 years and a fine of upto 3000 USD. CALL (877) 409-3489 (Toll Free).

Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

User name
Password
 Remember my credentials

OK Cancel

Call for support:
(877) 409-3489

Find downloads

I need help with...



Windows



Windows Phone 8



Lumia devices



Xbox



Office



OneDrive



Surface



Microsoft Edge



Internet Explorer



Skype



Outlook.com



MSN

Phishing is everywhere

IT'S UP TO YOU

Phishing most often plays on fear.
Other potential examples include:

- FedEx, UPS, USPS, Amazon failed delivery notices
- Coupons / Sales
- Voicemails
- Fax notices
- Fake invoices
- Overdue notices
- Fake account compromised notices
- Fake encrypted email notices
- Social media themed



BUT WAIT, THERE'S MORE!!

Social Engineering



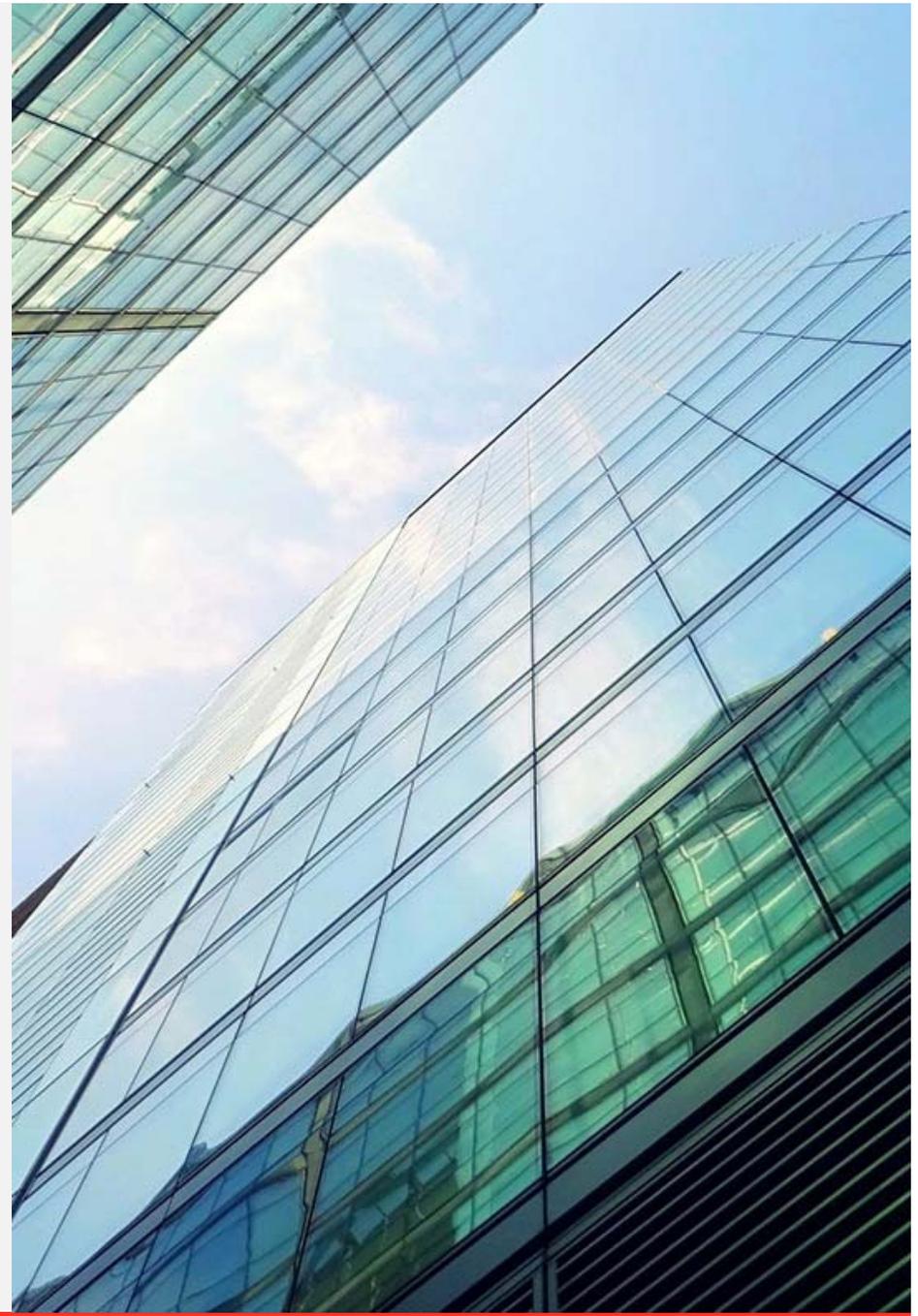
WHAT CAN I DO?

Never Assume



Firewalls cannot block all viruses

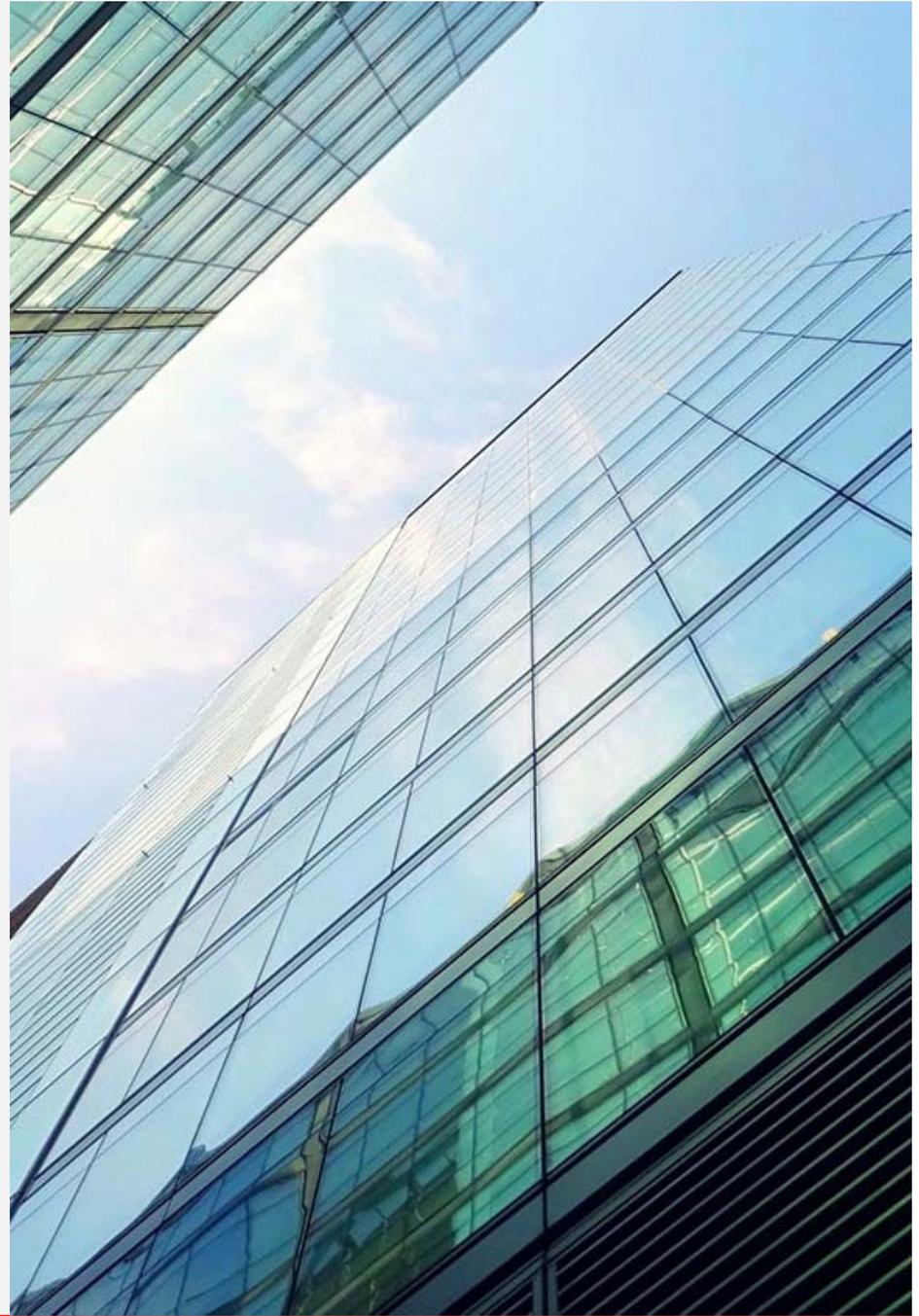
- The primary purpose of a firewall is to route traffic and to prevent unauthorized outside access to a network.
- Firewalls have added malware scanning but they are always a step behind.
- Next generation firewalls are using AI to help prevent viruses but they are currently very expensive.





Spam filters can only do so much

- Spam filters are starting to scan for advanced threats but you need to pay for that upgraded service.
- Advanced threat services are not guaranteed to eliminate all of the threats
- Most spam filters will not read deep into links
- Users get annoyed when a spam filter catches too much



NOW YOU KNOW

What can you do?

Email Policy

EDUCATION IS CRITICAL

Email was not designed to be a secure means of communication

Email not only serves as an easy way to steal outgoing sensitive information, it also serves as a way into your network.

1

Phishing attacks are at an all-time high. Employees should not be clicking links or opening attachments unless they are 100% sure the email is legitimate.

2

We live in a social media world, spear phishing attacks are extremely common.

3

Do not email sensitive information unless it is encrypted.

Security Starts With You

IT'S ONLY THE BEGINNING

Continuous Education

Humans are the weak link when it comes to security.

Humans can and will bypass security, sometimes unknowingly.

1

Question every email

2

Question every popup

3

Never be afraid to ask

Question Every Email

TAKE A DEEP BREATH

We are all busy and trying to work quickly.

It is important that you also work efficiently.

1

Read the email multiple times.

Look for:

- Spelling mistakes
- Grammar mistakes
- Calls to action
- Threatening language

2

Learn the power of the mouse hovering over a link

Does the link even make sense?

3

Hit reply to, does the email go to the correct person?

Question Every Attachment

TAKE A DEEP BREATH

We are all busy and trying to work quickly.

Slow down and review the attachment. One wrong click can cause network outages and downtime.

1

Read the email multiple times.

Look for:

- Spelling mistakes
- Grammar mistakes
- Calls to action
- Threatening language

2

Does the attachment have a link in it requiring an additional step?

In most cases any links are a red flag and should not be clicked without asking a system administrator for input/

3

Does the attachment ask you to enable macros?

DO NOT DO THIS!

Do You Have Doubts?

ASK

Never reply to an email asking for confirmation.

If the email account has been compromised you will get a confirmation that the email is safe to open.

Don't be fooled!

1

Pick up the phone and call the sender to verify the email is legitimate.

2

Ask a system administrator to review the email before opening. It can wait.

3

Assume the email is not legitimate.

MIND BLOWN

Final Thoughts

Continuous Improvement Required

TECHNOLOGY IS NOT “SET IT
AND FORGET IT”

Technology changes rapidly and requires daily, monthly, and yearly review.

A business leverages technology in many different ways. As the use of technology advances in your business, it is critical you evaluate each addition along the way.

1

24/7 Monitoring

- Antivirus/Malware Protection
- Operating System Updates
- File Access
- Employee Access
- Vendor Access
- Backup

2

Annual Risk Assessments

- Penetration Testing
- Employee Education Standards
- Policy Changes

3

Review

- Audit File Permissions
- Audit Group Policy (passwords, drive mapping, group membership)

THANK YOU

Questions?