Archdiocese of Seattle

INFORMATION TECHNOLOGY – PAA DAYS – BREAKOUT SESSION

MARCH 19, 2025

Information Technology Considerations for Parish Leaders

Topics

Cybersecurity
- Identification of online threats.
- Case Studies – Observations of Recent Hack Attempts
- Token Theft

Threats
- Global Threats
- Email Security
- Account Security
- Windows 10

Security Awareness Training

AOS Technology Summit 2025

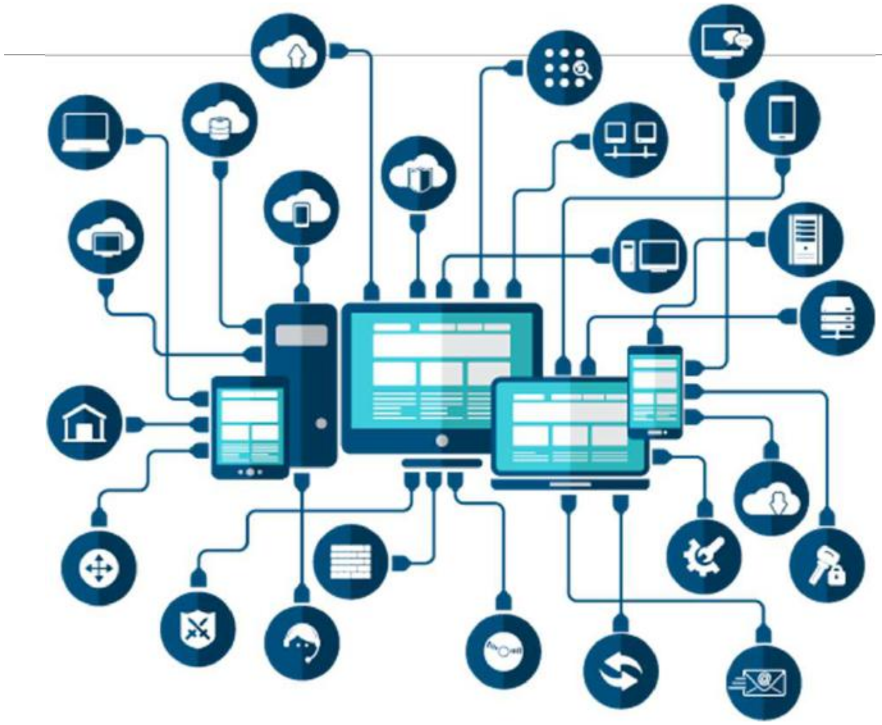
AOS-Share

AOS-365

Kevin's Q&A

AOS-365 – Technical with Caleb Dietzel

The Information Technology Landscape



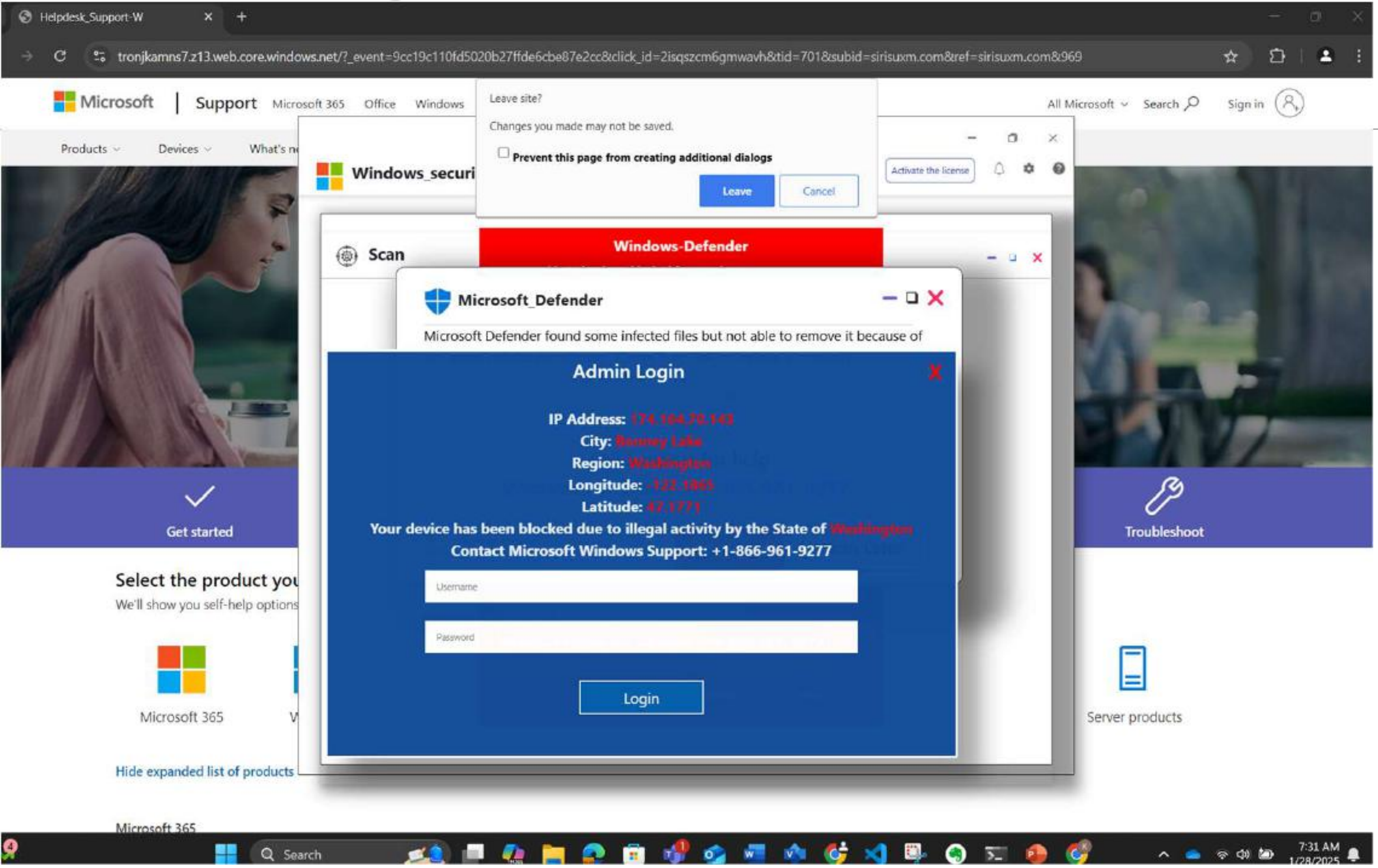
Routers,
Switches,
Desktop Computers,
Laptop Computers,
Servers,
Printers,
Firewalls…..

The Information Technology Landscape

68% of all computer breaches have a human that participated in the breach.

The most important thing you can do to protect your compute environment is to educate your users.

Understanding Threats



Helpdesk_Support-W

tronjkamns7.z13.web.core.windows.net/?_event=9cc19c110fd5020b27ffde6cbe87e2cc&click_id=2isqszcm6gmwavh&tid=701&subid=sirisuxm.com&ref=sirisuxm.com&969

Microsoft | Support Microsoft 365 Office Windows
All Microsoft Search Sign in
Products Devices What's n
Get started
Troubleshoot

Leave site?

Changes you made may not be saved.

□ Prevent this page from creating additional dialogs

Leave Cancel

Windows_securi
Activate the license
Scan

Windows-Defender

Microsoft_Defender

Microsoft Defender found some infected files but not able to remove it because of

Admin Login

IP Address: 174.104.70.143
City: Bonney Lake
Region: Washington
Longitude: -122.1865
Latitude: 47.1771
Your device has been blocked due to illegal activity by the State of Washington
Contact Microsoft Windows Support: +1-866-961-9277

Username

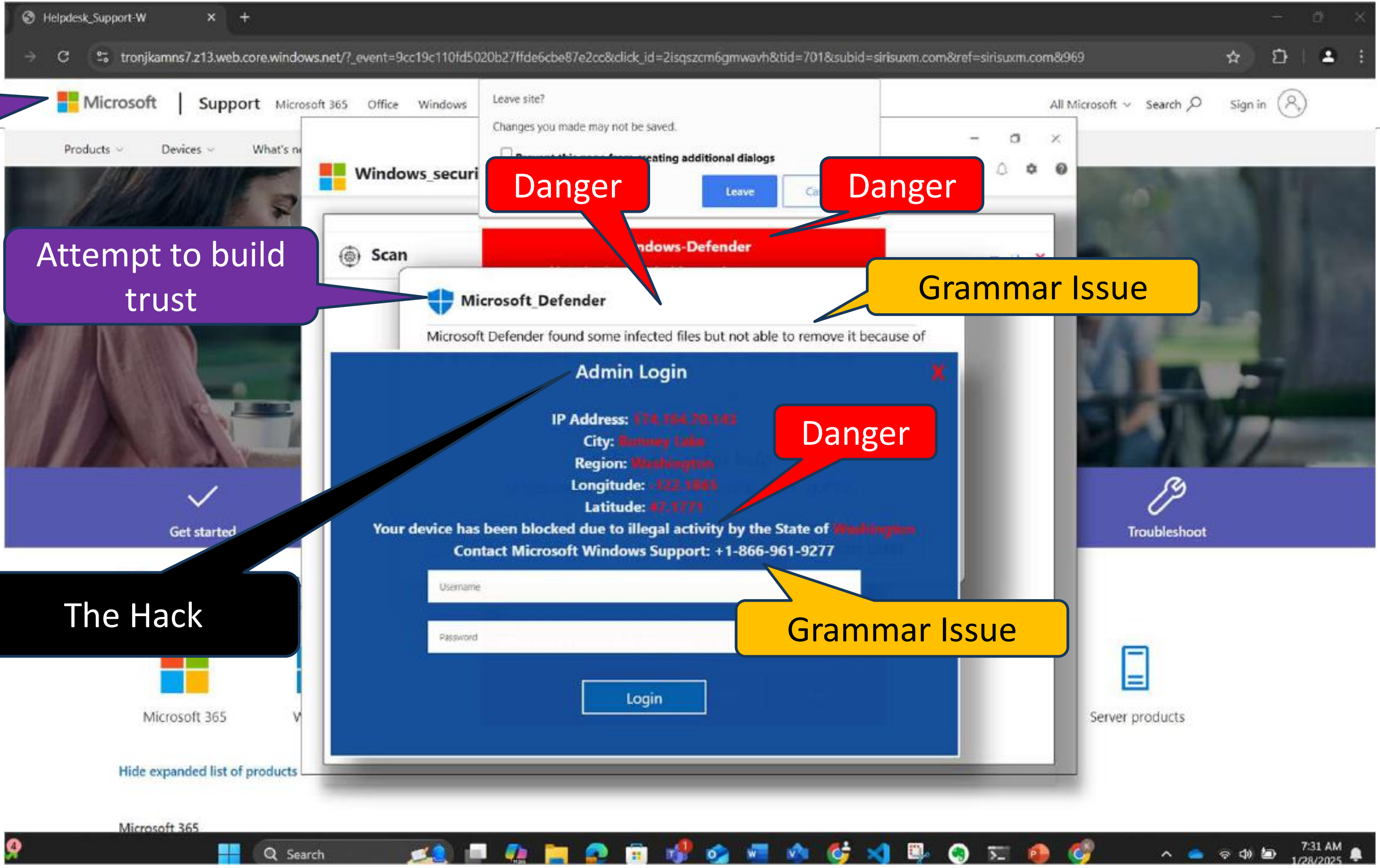
Password

Login

Select the product you

We'll show you self-help options

Understanding Threats - Scareware



Helpdesk_Support-W
tronjkamns7.z13.web.core.windows.net/?_event=9cc19c110fd5020b27ffde6cbe87e2cc&click_id=2isqszcm6gmwavh&tid=701&subid=sirisuxm.com&ref=sirisuxm.com&969
Microsoft | Support Microsoft 365 Office Windows
All Microsoft Search Sign in
Products Devices What's n
Windows_securi
Scan
Get started
Troubleshoot
Microsoft 365
Server products
Hide expanded list of products
Microsoft 365
Search
7:31 AM
1/28/2025

Leave site?

Changes you made may not be saved.

□ Prevent this page from creating additional dialogs

Leave | Ca

ndows-Defender

Microsoft_Defender

Microsoft Defender found some infected files but not able to remove it because of

Admin Login

IP Address: [redacted]
City: [redacted]
Region: [redacted]
Longitude: [redacted]
Latitude: [redacted]

Your device has been blocked due to illegal activity by the State of [redacted]

Contact Microsoft Windows Support: +1-866-961-9277

Username

Password

Login

Attempt to build trust

Attempt to build trust

Danger

Danger

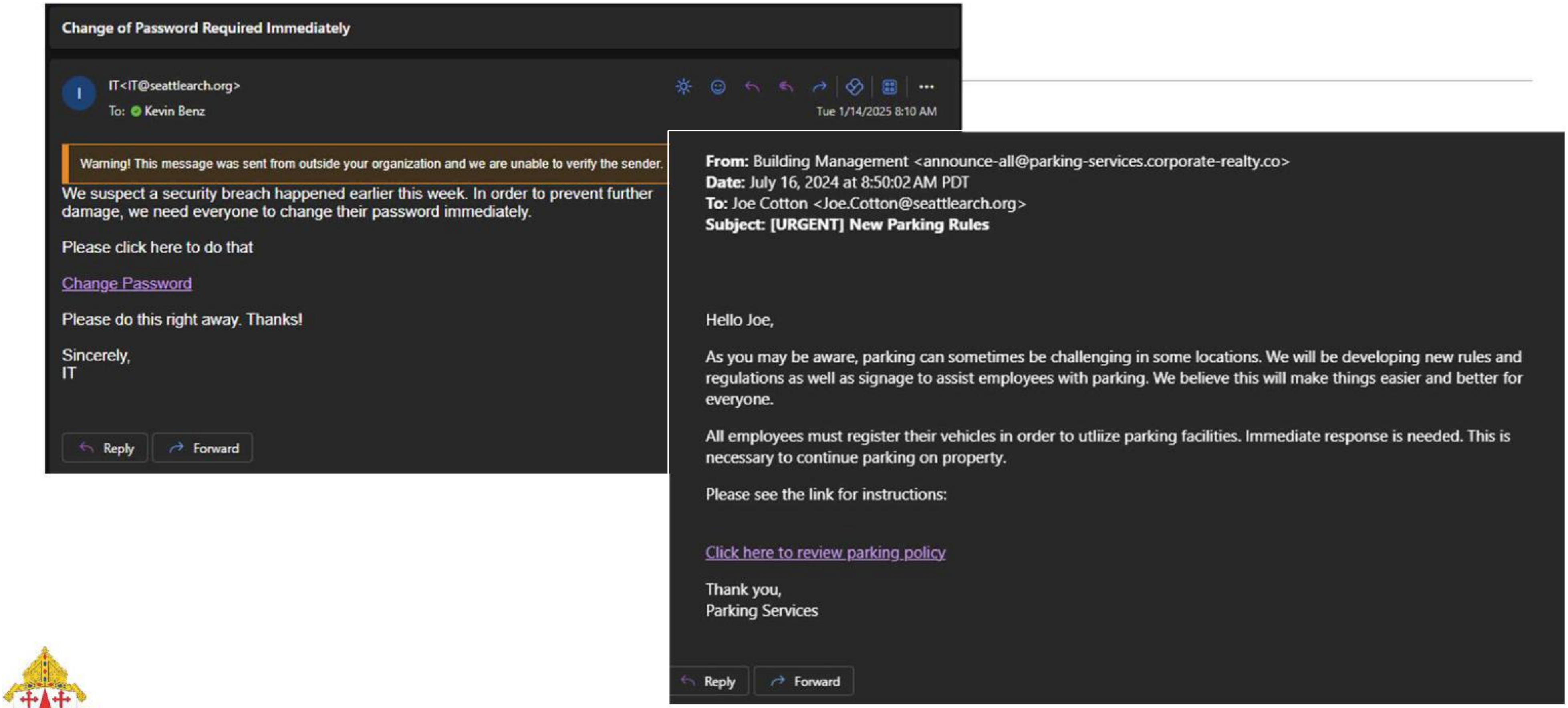
Danger

Grammar Issue

Grammar Issue

The Hack

Information Technology - Risks



Change of Password Required Immediately

IT<IT@seattlearch.org>

To: Kevin Benz

Tue 1/14/2025 8:10 AM

Warning! This message was sent from outside your organization and we are unable to verify the sender.

We suspect a security breach happened earlier this week. In order to prevent further damage, we need everyone to change their password immediately.

Please click here to do that

Change Password

Please do this right away. Thanks!

Sincerely,
IT

From: Building Management <announce-all@parking-services.corporate-realty.co>
Date: July 16, 2024 at 8:50:02 AM PDT
To: Joe Cotton <Joe.Cotton@seattlearch.org>
Subject: [URGENT] New Parking Rules

Hello Joe,

As you may be aware, parking can sometimes be challenging in some locations. We will be developing new rules and regulations as well as signage to assist employees with parking. We believe this will make things easier and better for everyone.

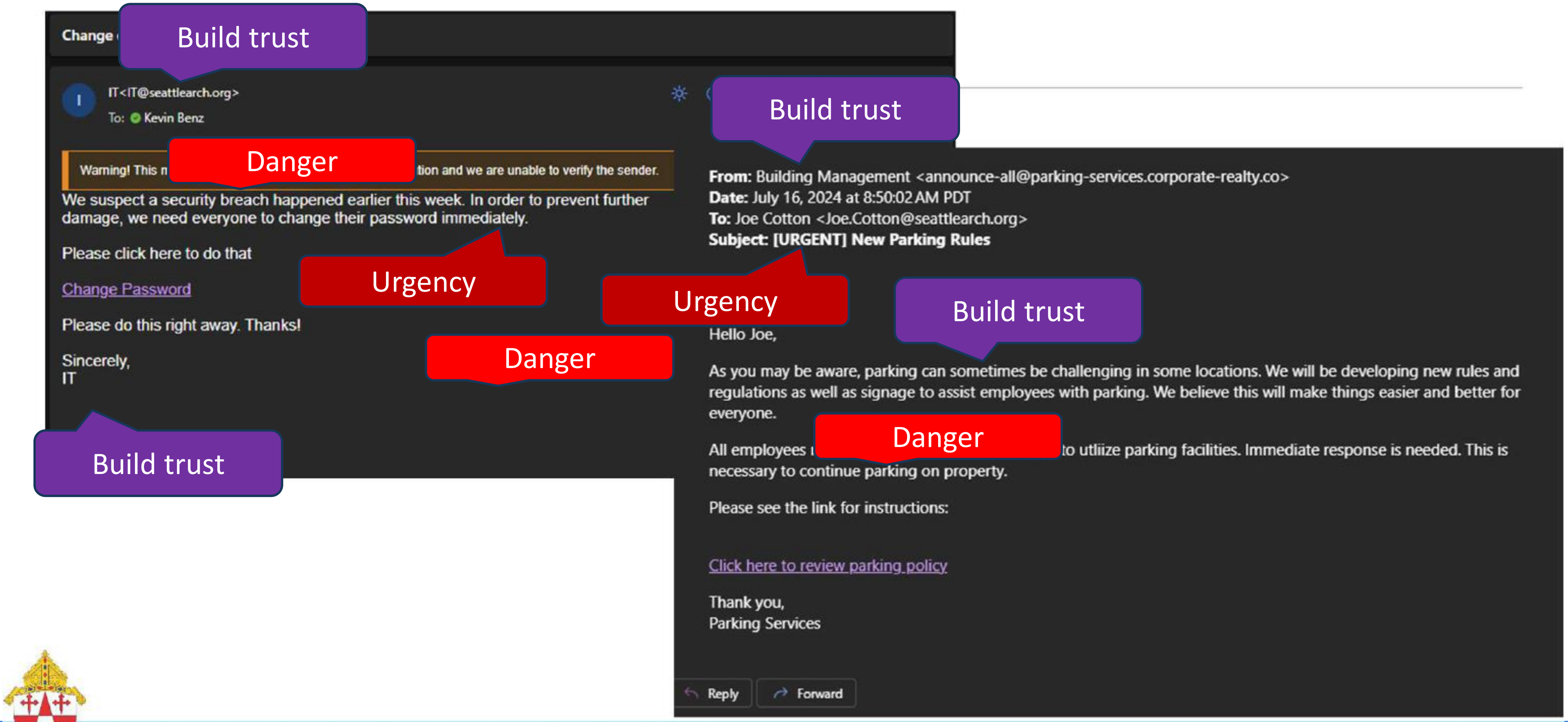
All employees must register their vehicles in order to utliize parking facilities. Immediate response is needed. This is necessary to continue parking on property.

Please see the link for instructions:

Click here to review parking policy

Thank you,
Parking Services

Information Technology - Risks



Change

IT<IT@seattlearch.org>

To: Kevin Benz

Warning! This m tion and we are unable to verify the sender.

We suspect a security breach happened earlier this week. In order to prevent further damage, we need everyone to change their password immediately.

Please click here to do that

Change Password

Please do this right away. Thanks!

Sincerely,
IT

From: Building Management <announce-all@parking-services.corporate-realty.co>
Date: July 16, 2024 at 8:50:02 AM PDT
To: Joe Cotton <Joe.Cotton@seattlearch.org>
Subject: [URGENT] New Parking Rules

Hello Joe,

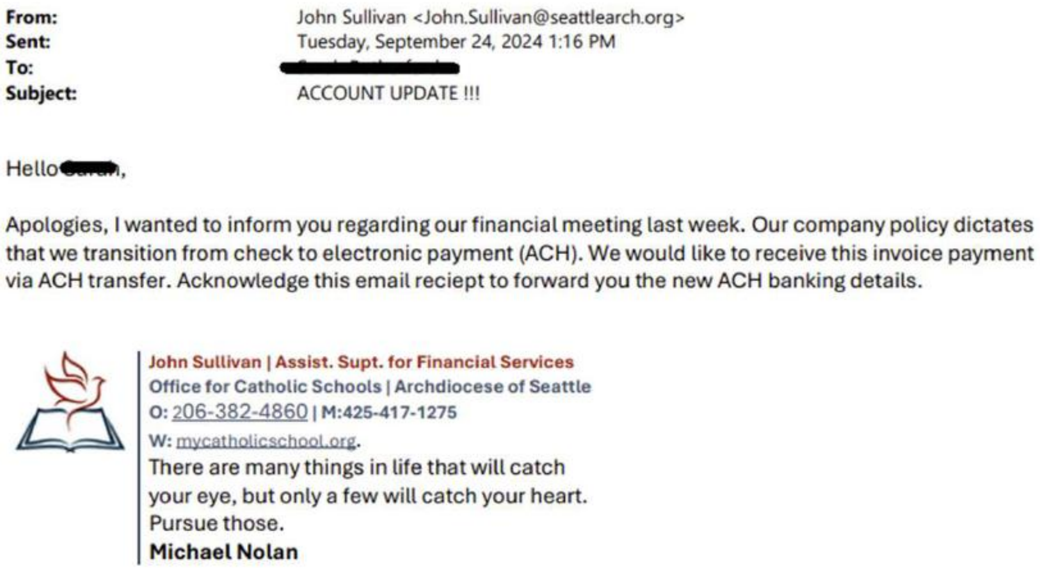
As you may be aware, parking can sometimes be challenging in some locations. We will be developing new rules and regulations as well as signage to assist employees with parking. We believe this will make things easier and better for everyone.

All employees to utliize parking facilities. Immediate response is needed. This is necessary to continue parking on property.

Please see the link for instructions:

Click here to review parking policy

Thank you,
Parking Services



From: John Sullivan <John.Sullivan@seattlearch.org>
Sent: Tuesday, September 24, 2024 1:16 PM
To: [redacted]
Subject: ACCOUNT UPDATE !!!

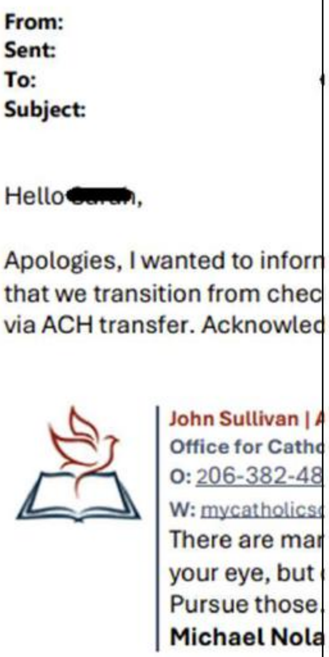
Hello [redacted],

Apologies, I wanted to inform you regarding our financial meeting last week. Our company policy dictates that we transition from check to electronic payment (ACH). We would like to receive this invoice payment via ACH transfer. Acknowledge this email reciept to forward you the new ACH banking details.

John Sullivan | Assist. Supt. for Financial Services
Office for Catholic Schools | Archdiocese of Seattle
O: 206-382-4860 | M:425-417-1275
W: mycatholicschool.org.
There are many things in life that will catch
your eye, but only a few will catch your heart.
Pursue those.
Michael Nolan

Exploration of a Hack

Exploration of a Hack – The Ask

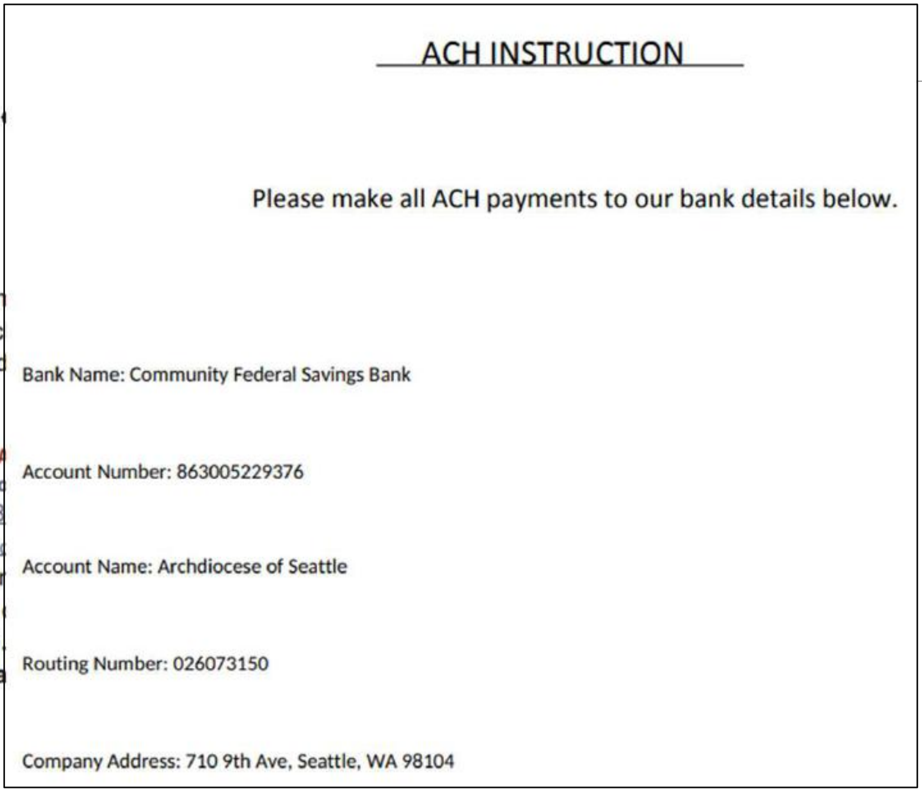


From:
Sent:
To:
Subject:

Hello [redacted],

Apologies, I wanted to inforn
that we transition from chec
via ACH transfer. Acknowled

John Sullivan | A
Office for Catho
O: 206-382-48
W: mycatholicsc
There are mar
your eye, but
Pursue those.
Michael Nola



ACH INSTRUCTION

Please make all ACH payments to our bank details below.

Bank Name: Community Federal Savings Bank

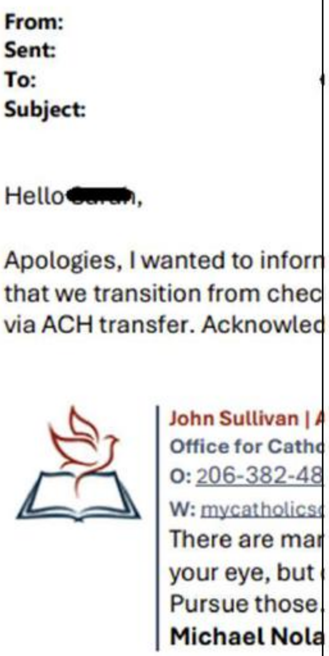
Account Number: 863005229376

Account Name: Archdiocese of Seattle

Routing Number: 026073150

Company Address: 710 9th Ave, Seattle, WA 98104

Exploration of a Hack

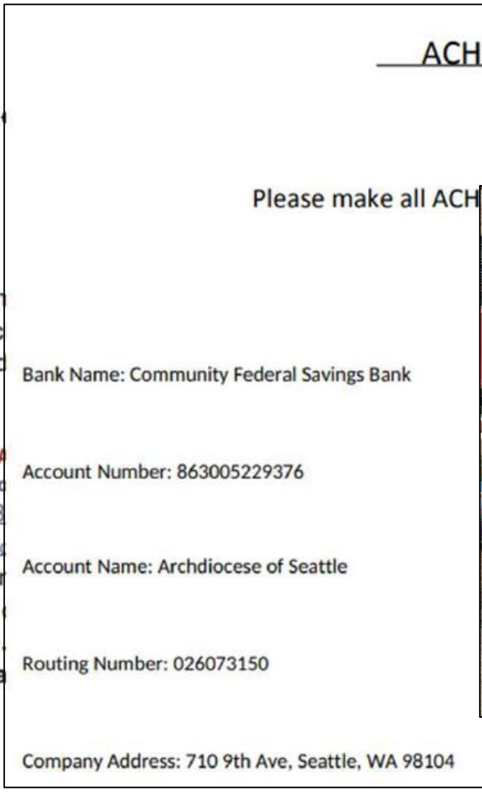


From:
Sent:
To:
Subject:

Hello [redacted],

Apologies, I wanted to inforn
that we transition from chec
via ACH transfer. Acknowled

John Sullivan | A
Office for Catho
O: 206-382-48
W: mycatholicsc
There are mar
your eye, but
Pursue those.
Michael Nola



ACH INSTRUCTION

Please make all ACH

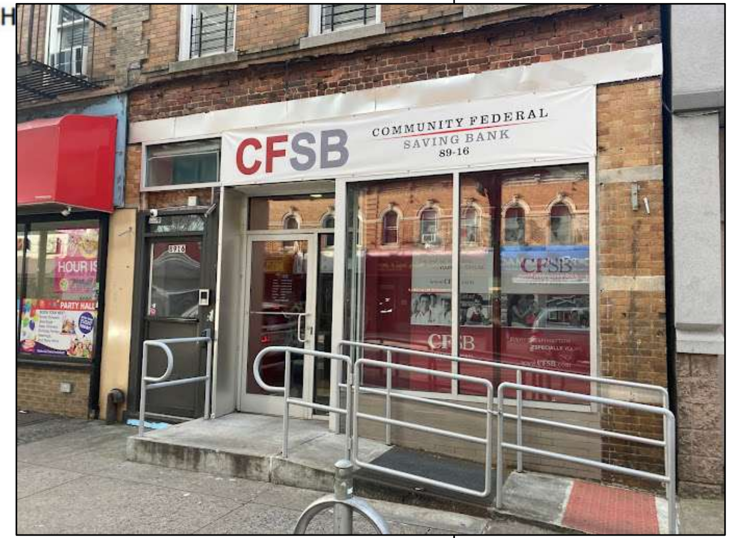
Bank Name: Community Federal Savings Bank

Account Number: 863005229376

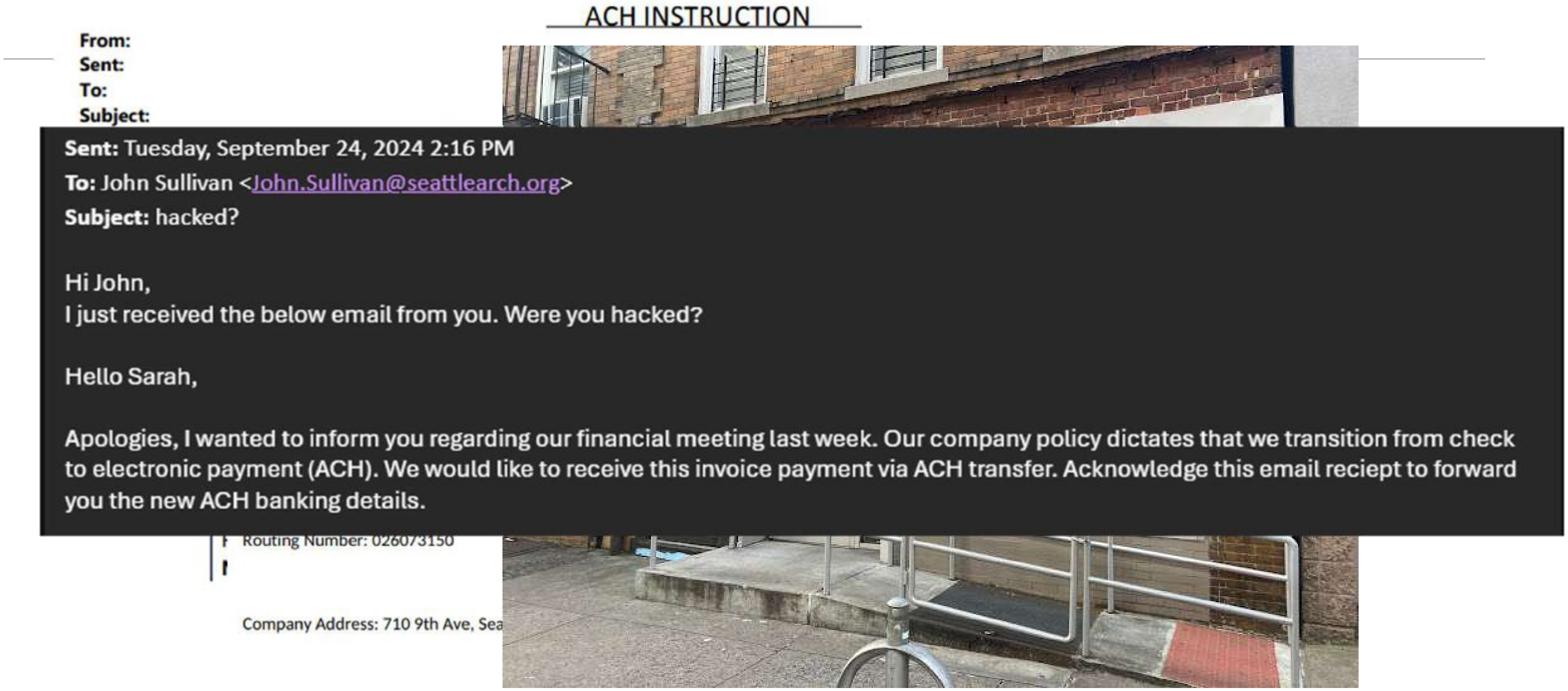
Account Name: Archdiocese of Seattle

Routing Number: 026073150

Company Address: 710 9th Ave, Seattle, WA 98104



Exploration of a Hack



ACH INSTRUCTION

From:
Sent:
To:
Subject:

Sent: Tuesday, September 24, 2024 2:16 PM
To: John Sullivan <John.Sullivan@seattlearch.org>
Subject: hacked?

Hi John,
I just received the below email from you. Were you hacked?

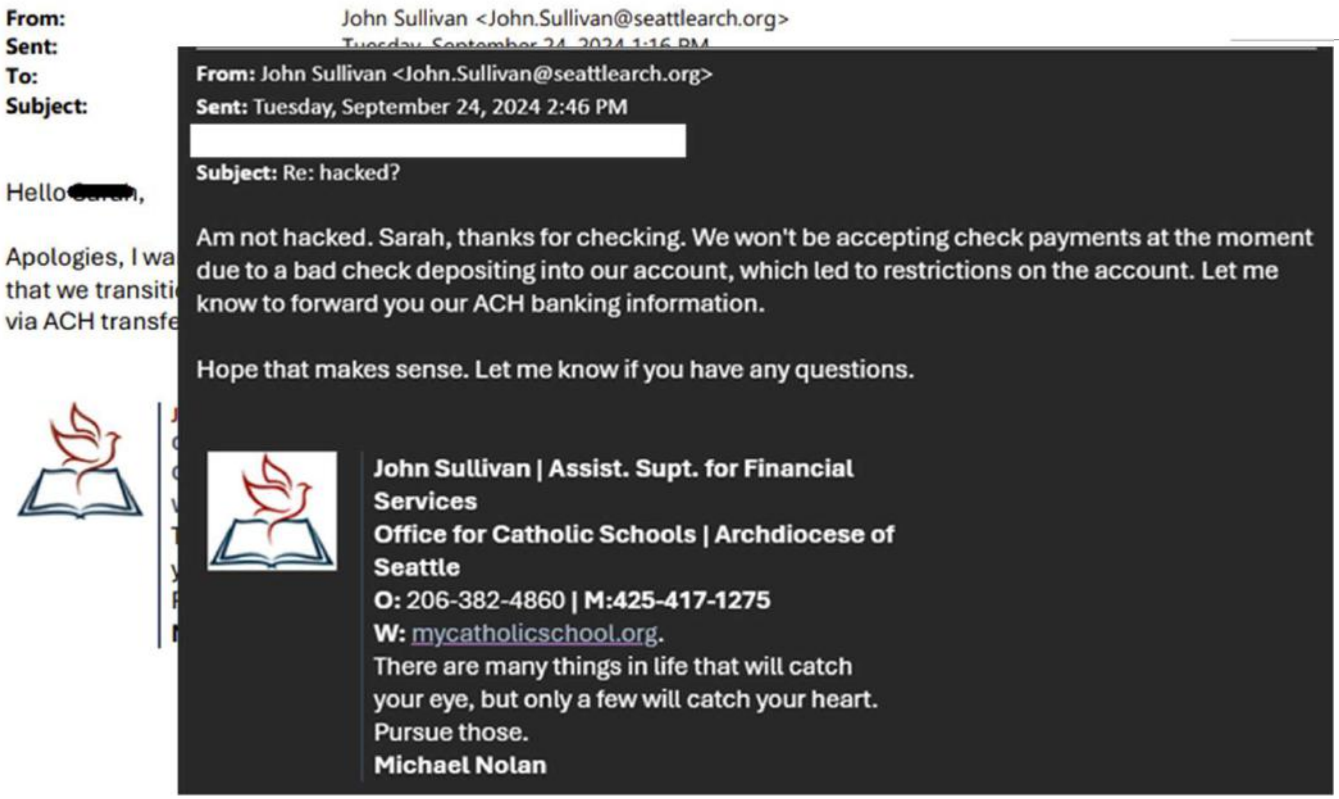
Hello Sarah,

Apologies, I wanted to inform you regarding our financial meeting last week. Our company policy dictates that we transition from check to electronic payment (ACH). We would like to receive this invoice payment via ACH transfer. Acknowledge this email reciept to forward you the new ACH banking details.

Routing Number: 026073150

Company Address: 710 9th Ave, Sea

Exploration of a Hack



From: John Sullivan <John.Sullivan@seattlearch.org>
Sent: Tuesday, September 24, 2024 1:16 PM
To:
Subject:

Hello[redacted],

Apologies, I wa
that we transiti
via ACH transfe

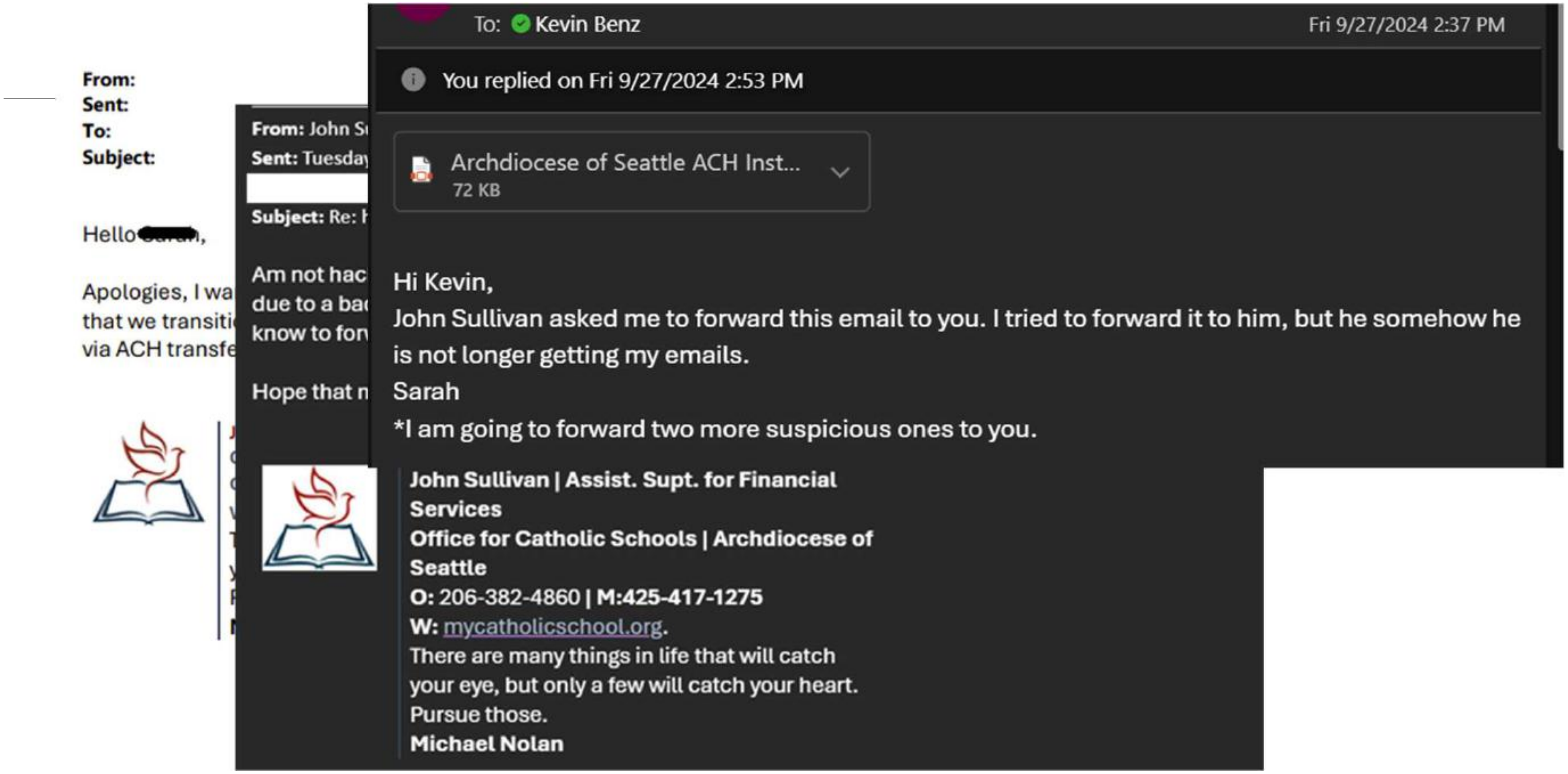
From: John Sullivan <John.Sullivan@seattlearch.org>
Sent: Tuesday, September 24, 2024 2:46 PM
[redacted]
Subject: Re: hacked?

Am not hacked. Sarah, thanks for checking. We won't be accepting check payments at the moment due to a bad check depositing into our account, which led to restrictions on the account. Let me know to forward you our ACH banking information.

Hope that makes sense. Let me know if you have any questions.

John Sullivan | Assist. Supt. for Financial Services
Office for Catholic Schools | Archdiocese of Seattle
O: 206-382-4860 | **M:425-417-1275**
W: mycatholicschool.org.
There are many things in life that will catch your eye, but only a few will catch your heart. Pursue those.
Michael Nolan

Exploration of a Hack



From:
Sent:
To:
Subject:

Hello[redacted],

Apologies, I wa
that we transiti
via ACH transfe

From: John S
Sent: Tuesday
Subject: Re: H

Am not hac
due to a ba
know to for

Hope that n

To: Kevin Benz

Fri 9/27/2024 2:37 PM

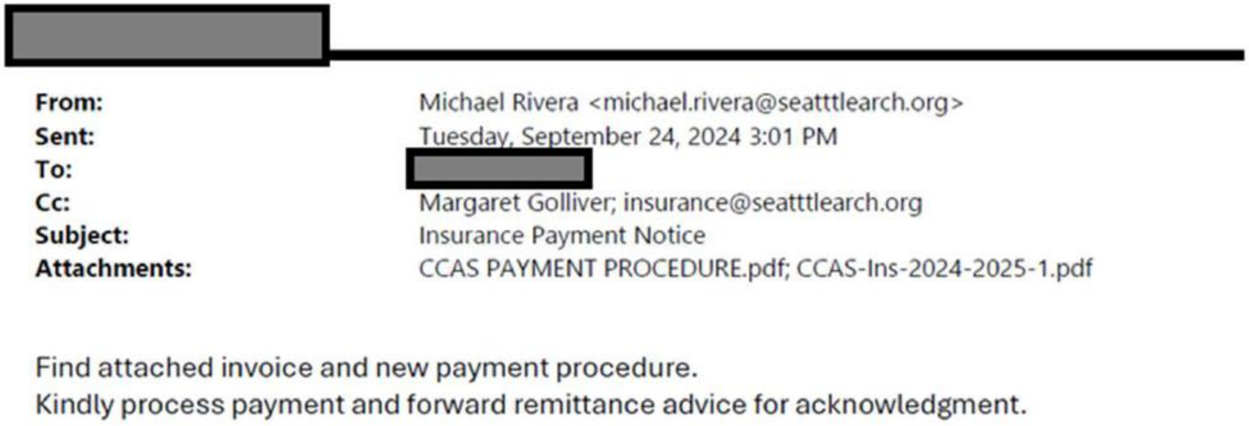
You replied on Fri 9/27/2024 2:53 PM

Archdiocese of Seattle ACH Inst...
72 KB

Hi Kevin,
John Sullivan asked me to forward this email to you. I tried to forward it to him, but he somehow he is not longer getting my emails.
Sarah
*I am going to forward two more suspicious ones to you.

John Sullivan | Assist. Supt. for Financial Services
Office for Catholic Schools | Archdiocese of Seattle
O: 206-382-4860 | **M:425-417-1275**
W: mycatholicschool.org.
There are many things in life that will catch your eye, but only a few will catch your heart. Pursue those.
Michael Nolan

Exploration of a Hack – Part Two

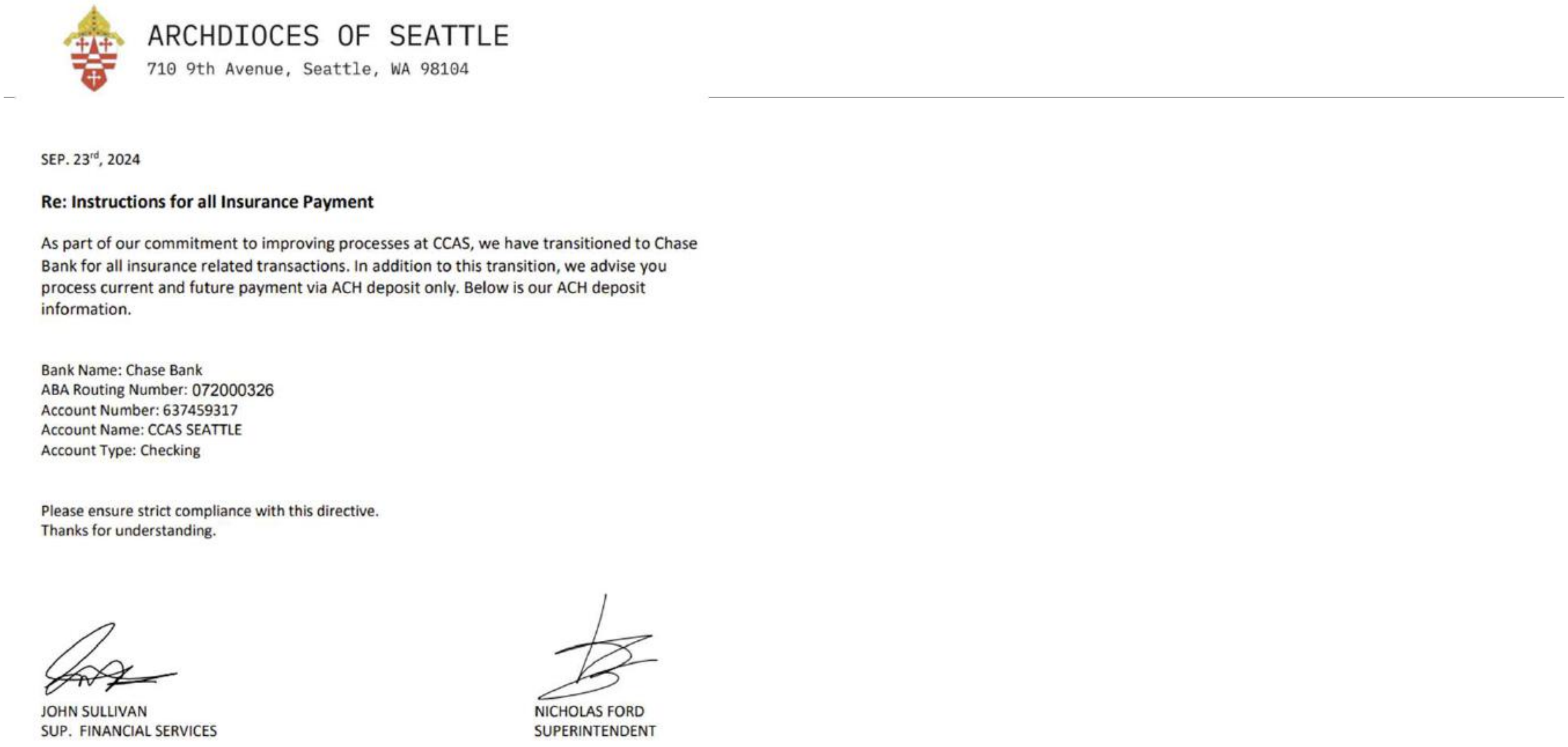


[redacted]

From: Michael Rivera <michael.rivera@seatttlearch.org>
Sent: Tuesday, September 24, 2024 3:01 PM
To: [redacted]
Cc: Margaret Golliver; insurance@seatttlearch.org
Subject: Insurance Payment Notice
Attachments: CCAS PAYMENT PROCEDURE.pdf; CCAS-Ins-2024-2025-1.pdf

Find attached invoice and new payment procedure.
Kindly process payment and forward remittance advice for acknowledgment.

Exploration of a Hack – Part Two



ARCHDIOCES OF SEATTLE
710 9th Avenue, Seattle, WA 98104

SEP. 23rd, 2024

Re: Instructions for all Insurance Payment

As part of our commitment to improving processes at CCAS, we have transitioned to Chase Bank for all insurance related transactions. In addition to this transition, we advise you process current and future payment via ACH deposit only. Below is our ACH deposit information.

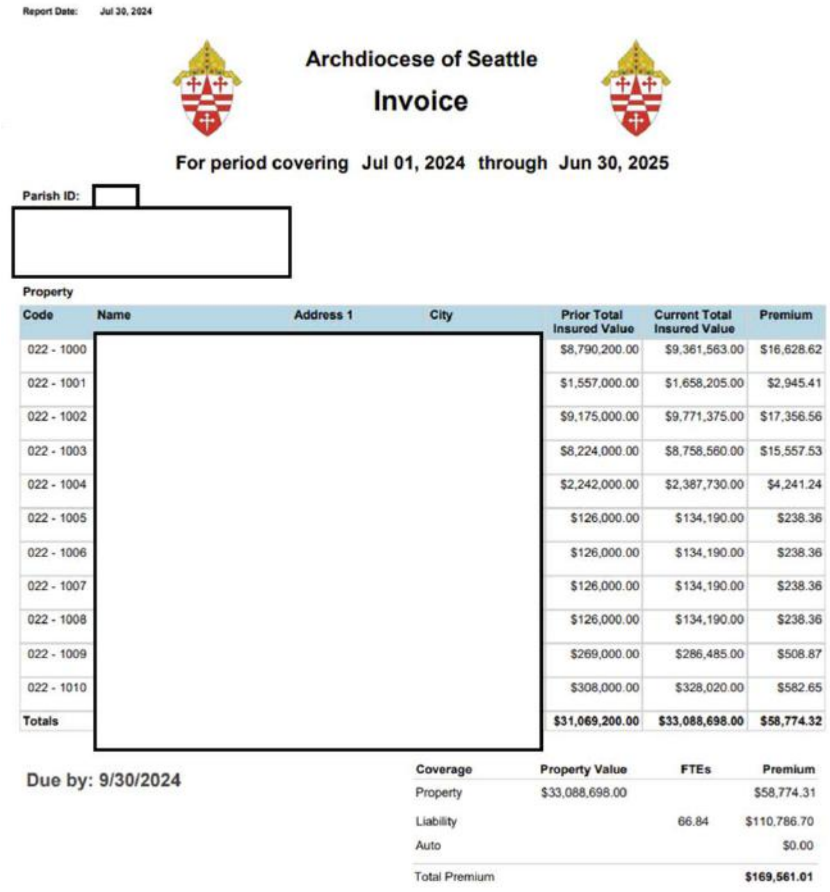
Bank Name: Chase Bank
ABA Routing Number: 072000326
Account Number: 637459317
Account Name: CCAS SEATTLE
Account Type: Checking

Please ensure strict compliance with this directive.
Thanks for understanding.

JOHN SULLIVAN
SUP. FINANCIAL SERVICES

NICHOLAS FORD
SUPERINTENDENT

Exploration of a Hack – Part Two



Report Date: Jul 30, 2024

Archdiocese of Seattle

Invoice

For period covering Jul 01, 2024 through Jun 30, 2025

Parish ID: [redacted]

[redacted]

Property

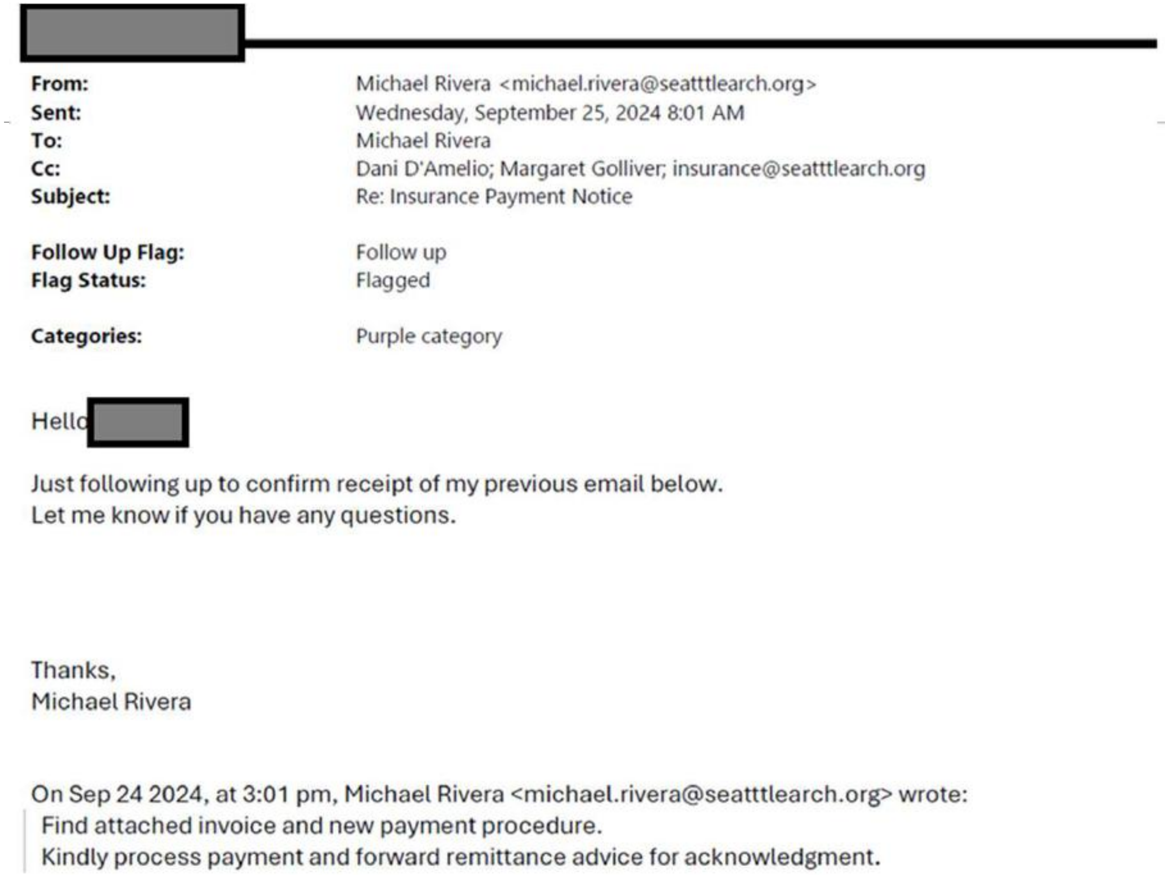
Code	Name	Address 1	City	Prior Total Insured Value	Current Total Insured Value	Premium
022 - 1000	[redacted]	[redacted]	[redacted]	$8,790,200.00	$9,361,563.00	$16,628.62
022 - 1001	[redacted]	[redacted]	[redacted]	$1,557,000.00	$1,658,205.00	$2,945.41
022 - 1002	[redacted]	[redacted]	[redacted]	$9,175,000.00	$9,771,375.00	$17,356.56
022 - 1003	[redacted]	[redacted]	[redacted]	$8,224,000.00	$8,758,560.00	$15,557.53
022 - 1004	[redacted]	[redacted]	[redacted]	$2,242,000.00	$2,387,730.00	$4,241.24
022 - 1005	[redacted]	[redacted]	[redacted]	$126,000.00	$134,190.00	$238.36
022 - 1006	[redacted]	[redacted]	[redacted]	$126,000.00	$134,190.00	$238.36
022 - 1007	[redacted]	[redacted]	[redacted]	$126,000.00	$134,190.00	$238.36
022 - 1008	[redacted]	[redacted]	[redacted]	$126,000.00	$134,190.00	$238.36
022 - 1009	[redacted]	[redacted]	[redacted]	$269,000.00	$286,485.00	$508.87
022 - 1010	[redacted]	[redacted]	[redacted]	$308,000.00	$328,020.00	$582.65
Totals	[redacted]	[redacted]	[redacted]	**$31,069,200.00**	**$33,088,698.00**	**$58,774.32**

Due by: 9/30/2024

Coverage	Property Value	FTEs	Premium
Property	$33,088,698.00		$58,774.31
Liability		66.84	$110,786.70
Auto			$0.00
Total Premium			**$169,561.01**

s
t

Exploration of a Hack – Part Two



[redacted]

From: Michael Rivera <michael.rivera@seatttlearch.org>
Sent: Wednesday, September 25, 2024 8:01 AM
To: Michael Rivera
Cc: Dani D'Amelio; Margaret Golliver; insurance@seatttlearch.org
Subject: Re: Insurance Payment Notice

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Purple category

Hello [redacted]

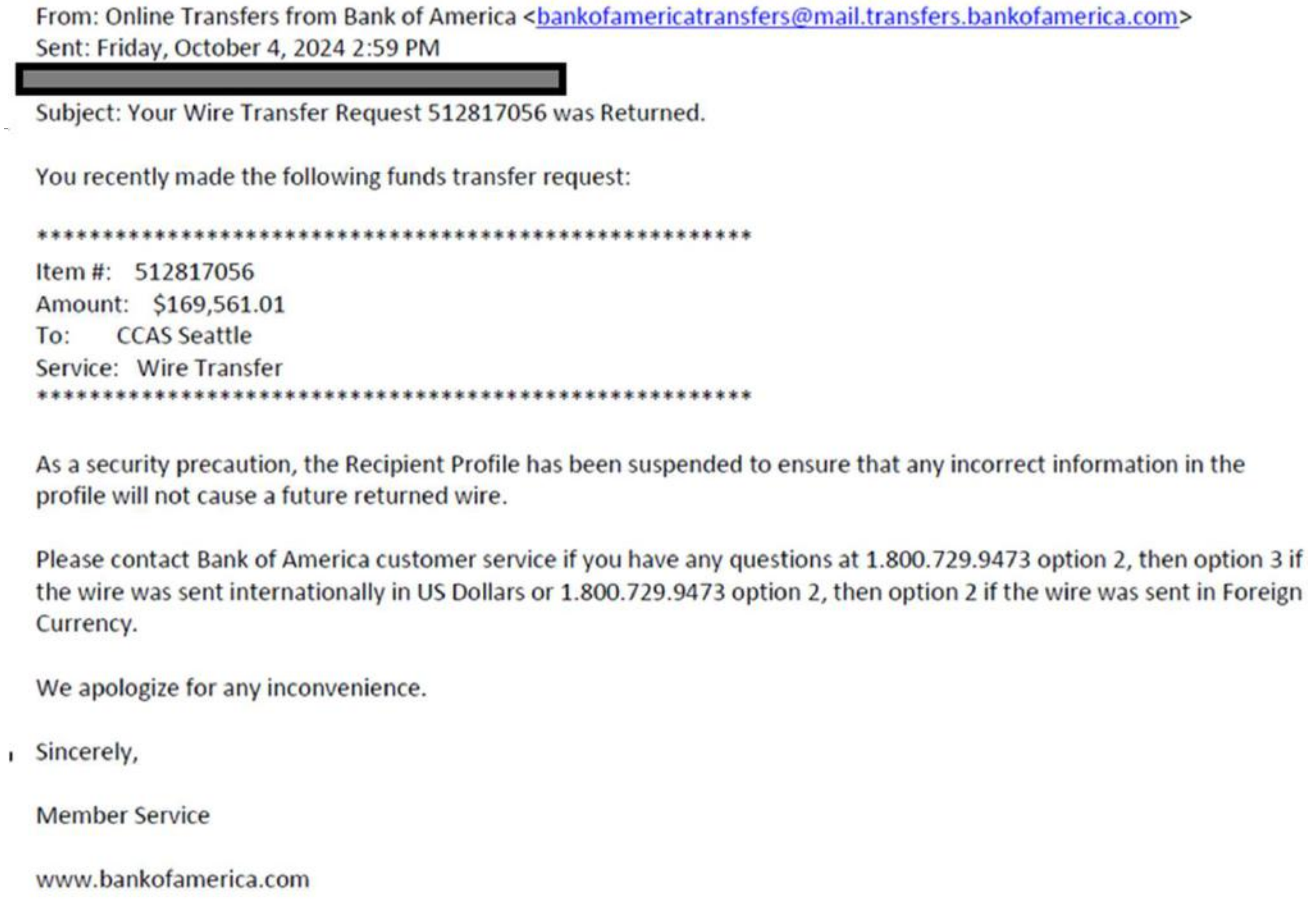
Just following up to confirm receipt of my previous email below.
Let me know if you have any questions.

Thanks,
Michael Rivera

On Sep 24 2024, at 3:01 pm, Michael Rivera <michael.rivera@seatttlearch.org> wrote:

> Find attached invoice and new payment procedure.
> Kindly process payment and forward remittance advice for acknowledgment.

Exploration of a Hack – Part Two



From: Online Transfers from Bank of America <bankofamericatransfers@mail.transfers.bankofamerica.com>
Sent: Friday, October 4, 2024 2:59 PM
[redacted]
Subject: Your Wire Transfer Request 512817056 was Returned.

You recently made the following funds transfer request:

****
Item #: 512817056
Amount: $169,561.01
To: CCAS Seattle
Service: Wire Transfer
****

As a security precaution, the Recipient Profile has been suspended to ensure that any incorrect information in the profile will not cause a future returned wire.

Please contact Bank of America customer service if you have any questions at 1.800.729.9473 option 2, then option 3 if the wire was sent internationally in US Dollars or 1.800.729.9473 option 2, then option 2 if the wire was sent in Foreign Currency.

We apologize for any inconvenience.

Sincerely,

Member Service

www.bankofamerica.com

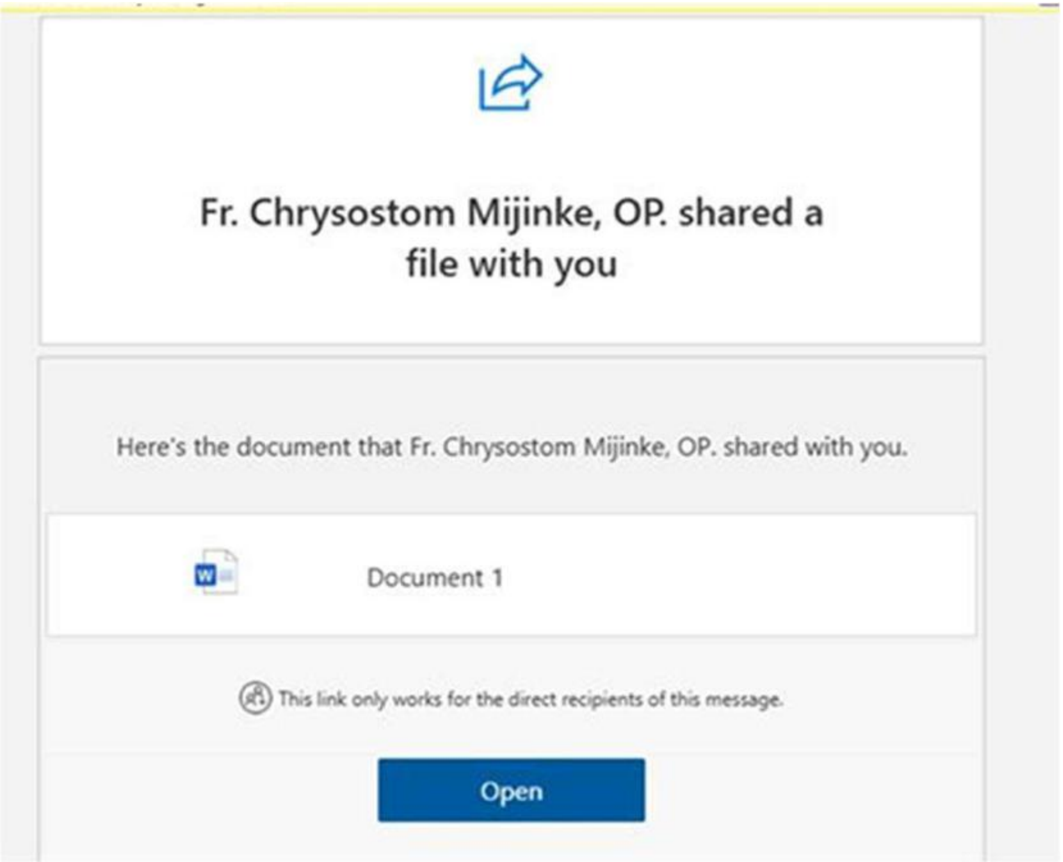
Critical Risk: 2FA Token Theft

By far the most serious exploit attempt we encounter, a successful token theft gives the hacker complete access to your identity and privileges.

When you click open, you're presented with an AOS login request and subsequent two-factor authorization.

When complete, the Hacker will have access to your Outlook, OneDrive, and every other O365 capability as well as every other system that utilizes O365 identity.

This email was received by 49 in the Chancery



Fr. Chrysostom Mijinke, OP. shared a file with you

Here's the document that Fr. Chrysostom Mijinke, OP. shared with you.

Document 1

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

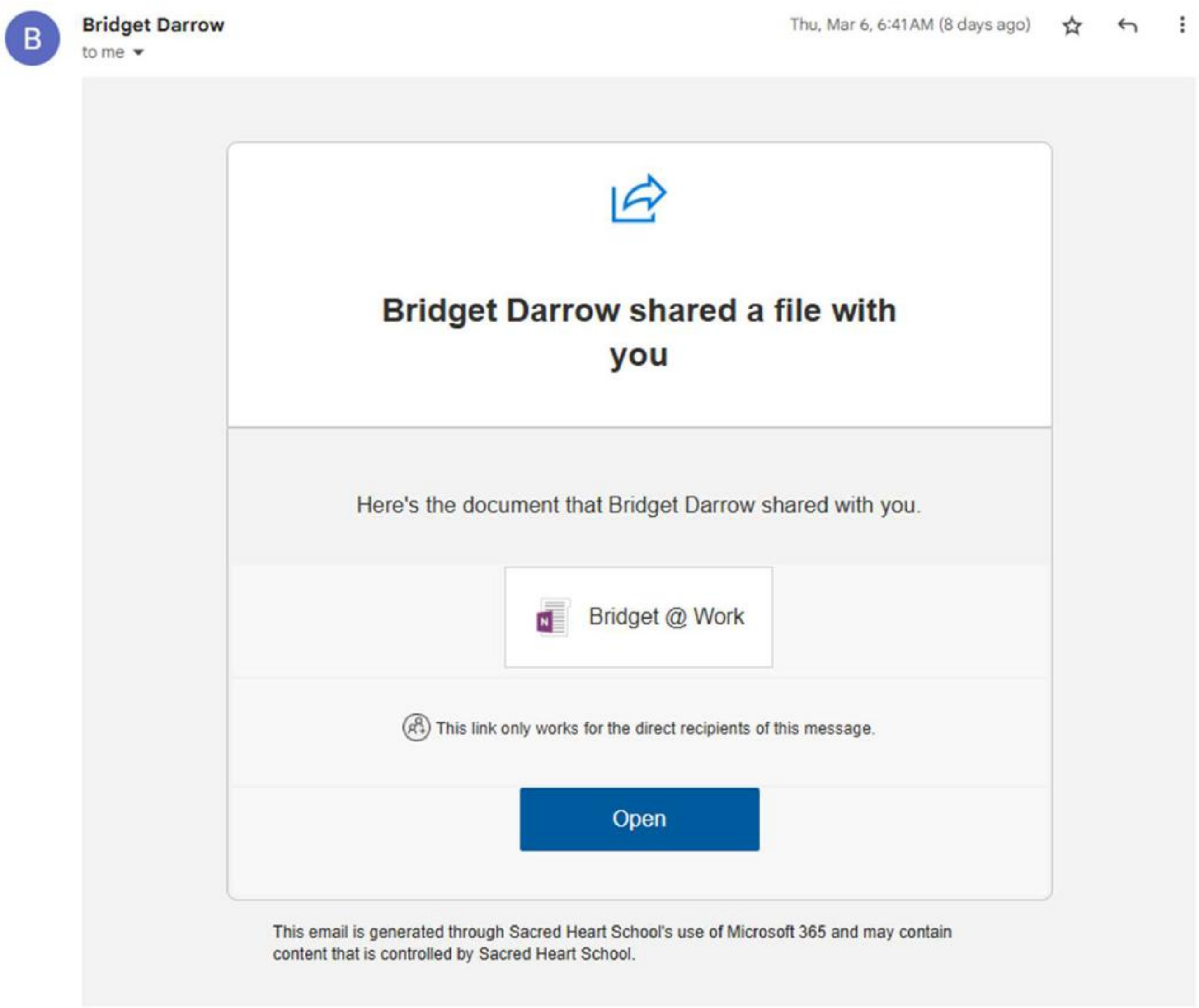
Critical Risk: 2FA Token Theft

By far the most serious exploit attempt we encounter, a successful token theft gives the hacker complete access to your identity and privileges.

When you click open, you're presented with an AOS login request and subsequent two-factor authorization.

When complete, the Hacker will have access to your Outlook, OneDrive, and every other O365 capability as well as every other system that utilizes O365 identity.

This email as sent to 510 people in Bridget's address book.



B

Bridget Darrow

to me

Thu, Mar 6, 6:41 AM (8 days ago)

Bridget Darrow shared a file with you

Here's the document that Bridget Darrow shared with you.

Bridget @ Work

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

Open

This email is generated through Sacred Heart School's use of Microsoft 365 and may contain content that is controlled by Sacred Heart School.

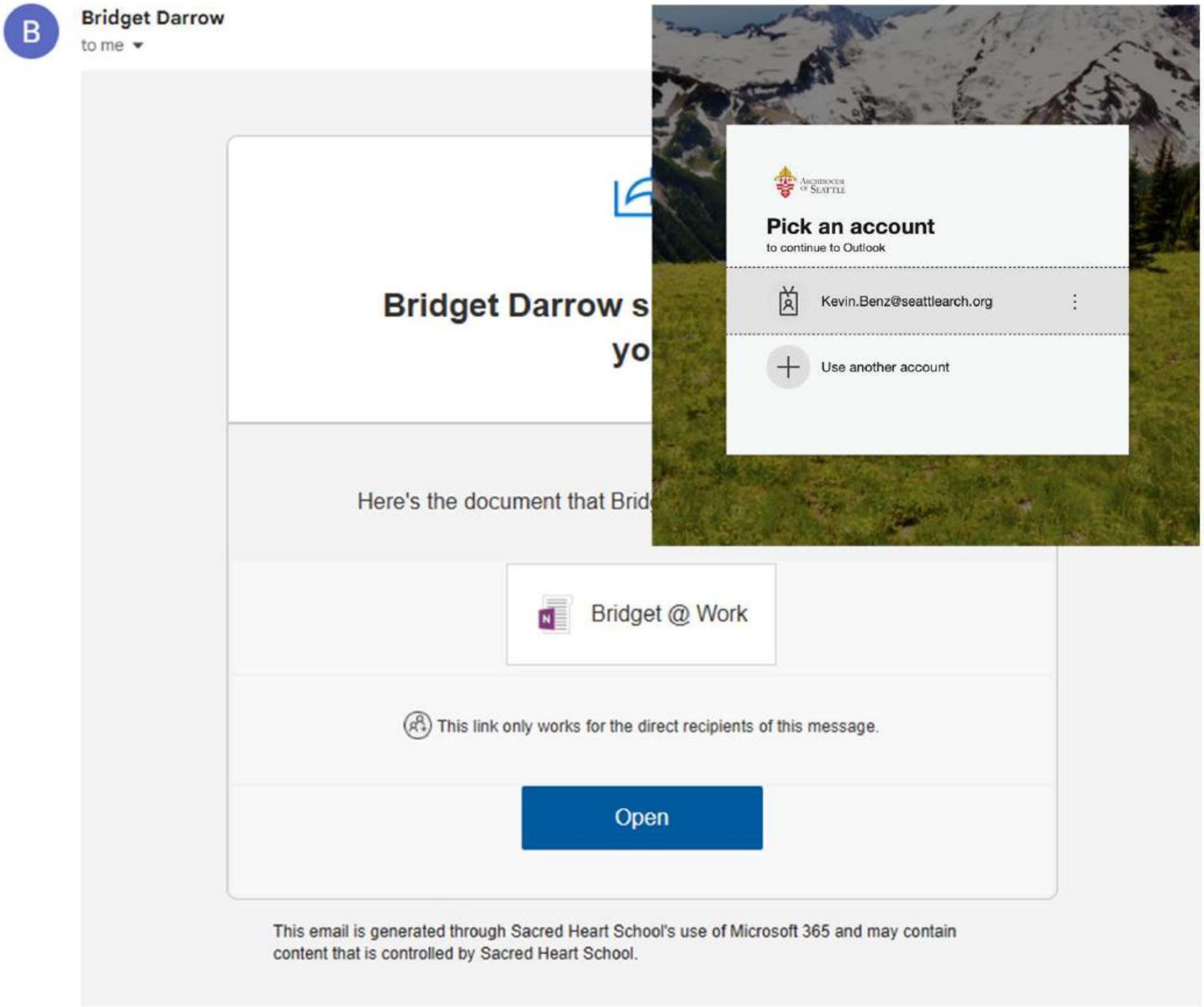
Critical Risk: 2FA Token Theft

By far the most serious exploit attempt we encounter, a successful token theft gives the hacker complete access to your identity and privileges.

When you click open, you're presented with an AOS login request and subsequent two-factor authorization.

When complete, the Hacker will have access to your Outlook, OneDrive, and every other O365 capability as well as every other system that utilizes O365 identity.

This email as sent to 510 people in Bridget's address book.



Bridget Darrow
to me

Bridget Darrow s
yo

Here's the document that Brid

Bridget @ Work

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

This email is generated through Sacred Heart School's use of Microsoft 365 and may contain content that is controlled by Sacred Heart School.

Pick an account
to continue to Outlook

Kevin.Benz@seattlearch.org

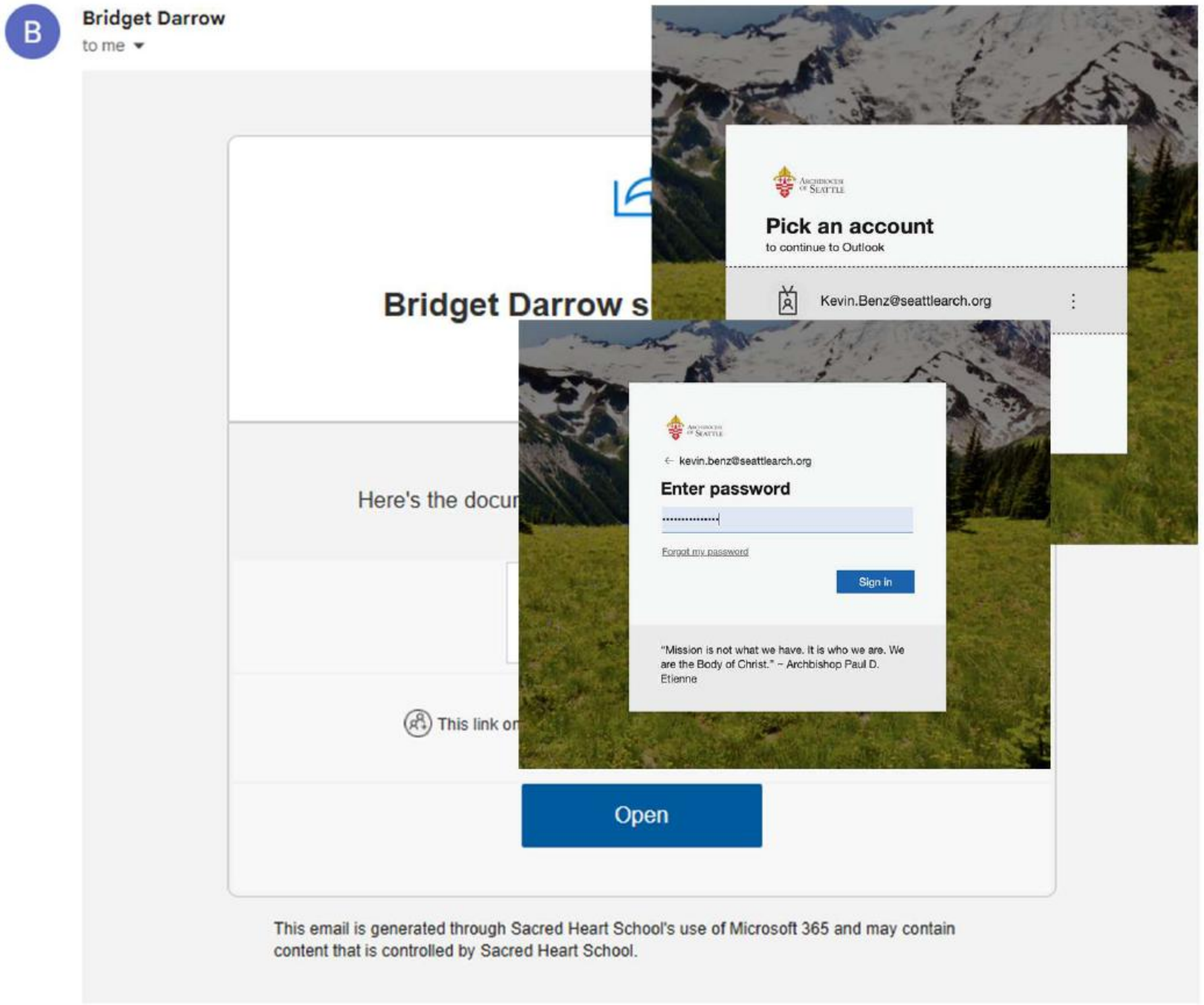
Critical Risk: 2FA Token Theft

By far the most serious exploit attempt we encounter, a successful token theft gives the hacker complete access to your identity and privileges.

When you click open, you're presented with an AOS login request and subsequent two-factor authorization.

When complete, the Hacker will have access to your Outlook, OneDrive, and every other O365 capability as well as every other system that utilizes O365 identity.

This email as sent to 510 people in Bridget's address book.



Bridget Darrow
to me

Bridget Darrow s

Here's the docu

This link o

Open

This email is generated through Sacred Heart School's use of Microsoft 365 and may contain content that is controlled by Sacred Heart School.

Pick an account
to continue to Outlook

Kevin.Benz@seattlearch.org

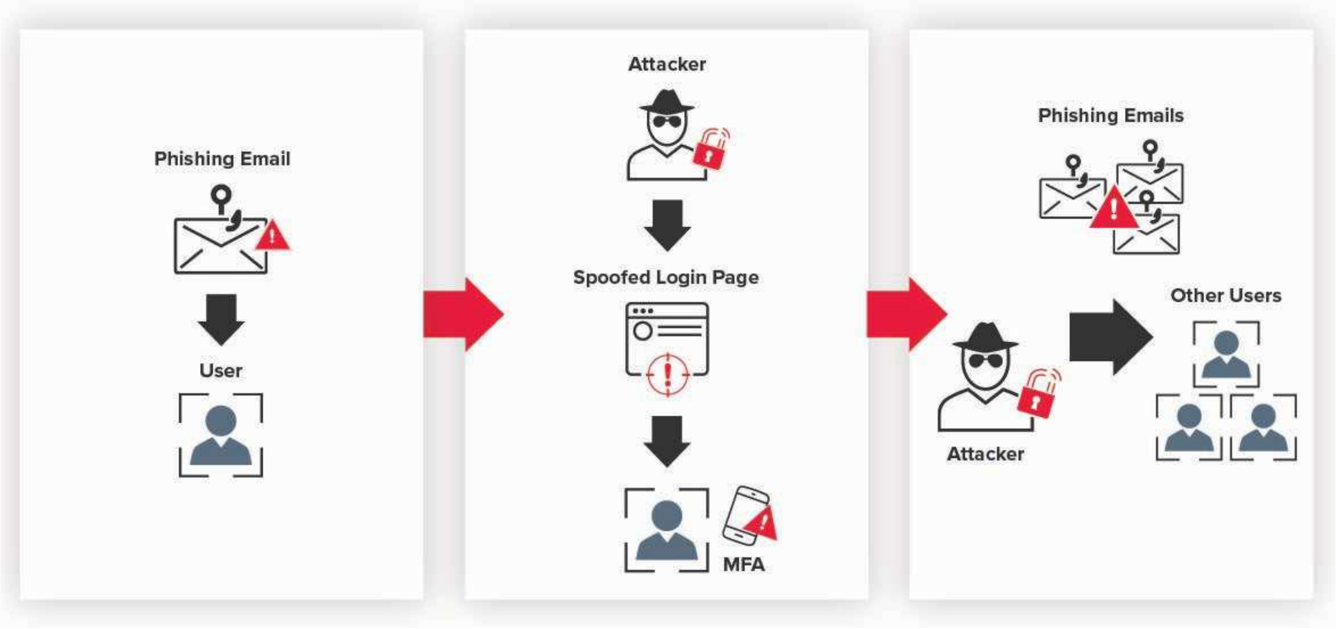
← kevin.benz@seattlearch.org

Enter password

Forgot my password

Sign in

"Mission is not what we have. It is who we are. We are the Body of Christ." – Archbishop Paul D. Etienne



If you’re not expecting the file, don’t open it.
Do not email the sender for verification, they have been exploited, and you will be interacting with the hacker.

INNOVATION > CYBERSECURITY

FBI Warning—Gmail, Outlook And VPN Users Need To Act Now

In partnership with the U.S. Cybersecurity and Infrastructure Security Agency, the FBI has issued a joint March 12 cybersecurity advisory against the backdrop of attacks by the Medusa ransomware group. The full FBI alert, AA25-071A, goes into great depth regarding the technicalities of the Medusa operation. As such, it is of importance that this should be read by all cyber-defenders. However, for the purposes of this article I am going to focus on the attack mitigation advice offered by the FBI.

Forbes

2025 GLOBAL THREAT REPORT

Here are a few key facts you should know about the shifting threat landscape:

- Breakout time — how long it takes for an adversary to start moving laterally across your network — reached an all-time low in the past year: The average fell to 48 minutes, and the fastest breakout time we observed dropped to a mere 51 seconds.
- Voice phishing (vishing) attacks, where adversaries call victims to amplify their activities with persuasive social engineering techniques, saw explosive growth — up 442% between the first and second half of 2024.
- Attacks related to initial access boomed, accounting for 52% of vulnerabilities observed by CrowdStrike in 2024. Providing access as a service became a thriving business, as advertisements for access brokers increased 50% year-over-year.
- Among nation-states, China-nexus activity surged 150% overall, with some targeted industries suffering 200% to 300% more attacks than the previous year.
- GenAI played a pivotal role in sophisticated cyberattack campaigns in 2024. It enabled FAMOUS CHOLLIMA to create highly convincing fake IT job candidates that infiltrated victim organizations, and it helped China-, Russia-, and Iran-affiliated threat actors conduct AI-driven disinformation and influence operations to disrupt elections.

Is Anti-Virus and Anti-Malware Enough?

While virus protection software can be effective in detecting and removing known malware, it's important to remember that no software is 100% foolproof, and a multi-layered approach to cybersecurity is crucial.

Here's a more detailed explanation:

- **Antivirus Software Works, But Isn't Perfect**
- **No Guarantee of 100% Protection:**
- **Multi-Layered Approach is Key:**
- **Keeping Software and Operating System Updated:**
- **Avoiding Risky Behavior:**
- **Strong Passwords and Two-Factor Authentication**
- **Data Backups:**
- **Be Aware of False Positives**
- **Antivirus Software Can't Protect Against All Online Risks:**

In conclusion: While antivirus software is a valuable tool in your cybersecurity arsenal, it's not a silver bullet. A multi-layered approach, including strong security habits and staying informed about online threats, is essential for protecting your devices and data.

Email Security

Verify the Email Sender.

Carefully examine the email sender
If in doubt, use a Parish directory to call the individual for confirmation of a received text or email. Do not use a phone number that may be provided in the body of the email.

Stop before clicking on a link
Hover over links in emails to ensure the link is legitimate. Or open a browser and type in the link manually

Be wary of email attachments
Do not open an attachment if you were not expecting one

Learn how to recognize a Phish
Messages that contain a high sense of urgency
A request for personal information (Social Security, password, etc.)
Poor writing or grammar

Account Security

Create a strong password

Strong password minimum 14 character with capitals/symbols/numbers

e.g. rol.led%SE-ALS7pools

Do not re-use passwords

Never share your Login information

Utilize a secure password manager such as e.g. 1Password

Enable 2FA/MFA

Try to use an authenticator app as a second verification and not an email/phone number

Google Auth, Microsoft Auth, etc.

Best Practice

Avoid selecting "Remember me" when logging into an account

Always log out of the website/computer if not in use

Try to update your password every 3 – 6 months

YouTube – Adobe

Amazon

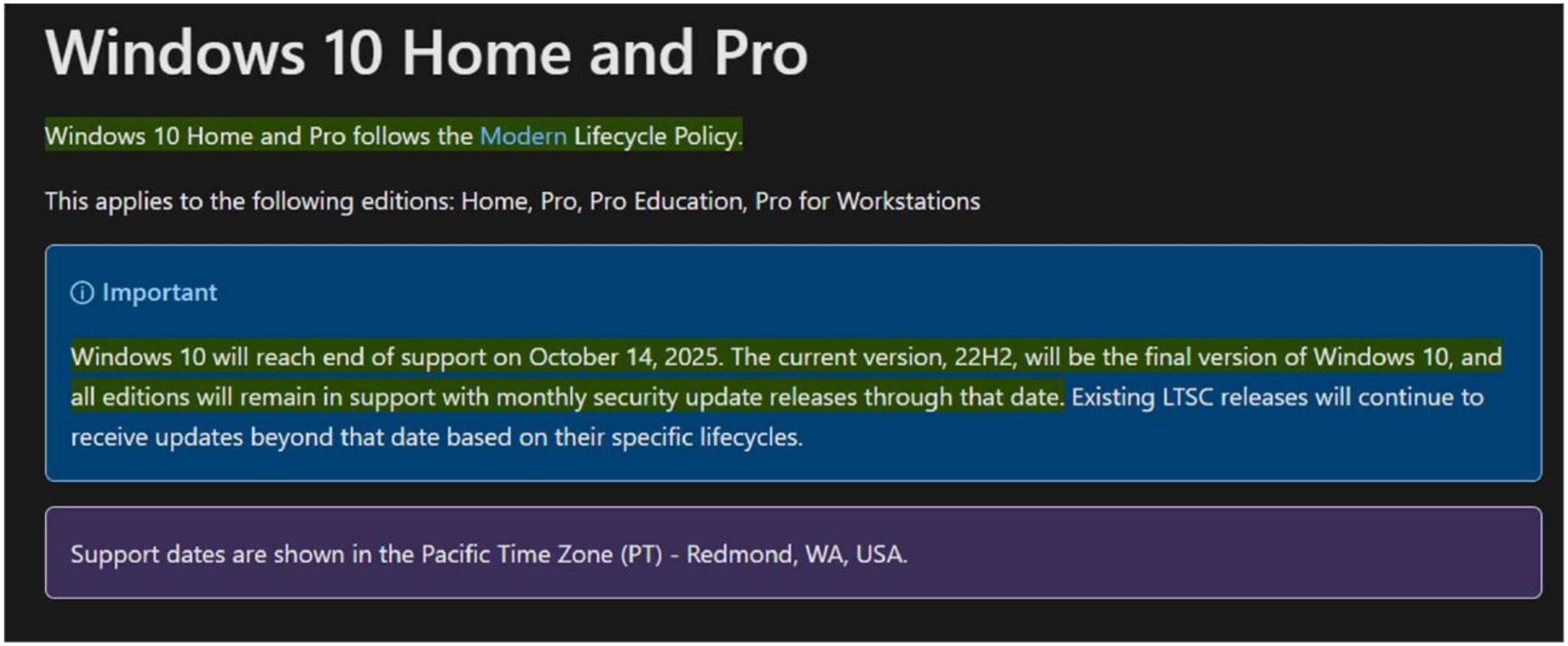
FTC.GOV

KnowB4

Free – Security Awareness Training Options
YouTube, Amazon & FTC

Paid – Security Awareness Training Options
KnowB4

Windows 10 – End of Life



Windows 10 Home and Pro

Windows 10 Home and Pro follows the Modern Lifecycle Policy.

This applies to the following editions: Home, Pro, Pro Education, Pro for Workstations

ⓘ Important

Windows 10 will reach end of support on October 14, 2025. The current version, 22H2, will be the final version of Windows 10, and all editions will remain in support with monthly security update releases through that date. Existing LTSC releases will continue to receive updates beyond that date based on their specific lifecycles.

Support dates are shown in the Pacific Time Zone (PT) - Redmond, WA, USA.

Archdiocese of Seattle – Technology Summit

Topic - Evolving Threat Landscape:

Cyber threats are constantly evolving, requiring us to stay vigilant and adapt our security measures accordingly.

Topic - Risks:

Ignoring information security issues can lead to significant financial losses, reputational damage, and operational disruptions.

Topic - Proactive Approach:

A proactive approach to cybersecurity is crucial for protecting our organization's valuable assets and data.

Topic - Collaboration and Knowledge Sharing:

This meeting will provide a platform for different teams to collaborate, share their knowledge, and develop a unified approach to cybersecurity.

What are worries you?

Announcing 2025 AOS Technology Summit

Planned for Spring 2025, this day will focus on the discussion of information technology issues in front of us.

Use this QR code to complete a survey about participation in the 2025 AOS Technology Summit. We are in the early stages of planning, and your feedback is critical as we envision what this event could be. Thank you in advance for your information. All feedback is a gift.

A New Way for Document Sharing

AOS-Share – “For Parishes SharePoint”

As part of the long-term strategy to improve the archdiocese’s use of technology, the Archdiocese of Seattle has built a new way to easily and securely share documents from the Chancery to parishes and schools. The IT team created a new secure online platform where registered employees can store and collaborate on content. AOS-Share offers improved efficiency, scalability and security by replacing many of the disjoined file-sharing sources, such as Box.com, DropBox.com, Google Docs, and the myriad collection of email attachments. In deploying AOS-Share, we will be enhancing collaboration, providing uniform content management and making it easier for everyone to share and access files.

Specifically, the AOS-Share platform will be organized with private folders for each parish family.

A New Way for Document Sharing

AOS-Share – "For Parishes SharePoint"

Currently, each of the folders has the following documents uploaded:

- Historical Property & Construction Files (blueprints, drawings, renderings)
- Parish Property Reports
- Partners in the Gospel Parish Viability Metrics and Workplan Templates

The key things to know about this tool are:

Only pastors, pastoral coordinators and identified pastoral assistant for administration and director of operations will have access to the SharePoint site, ensuring that the information is securely shared with the appropriate people.

We will provide you with the list of all people who will have SharePoint access for your parish family. (Note: If someone else from your team needs access, we will provide direction on how to update access permissions.)

AOS-365 Platform – Archdiocese of Seattle

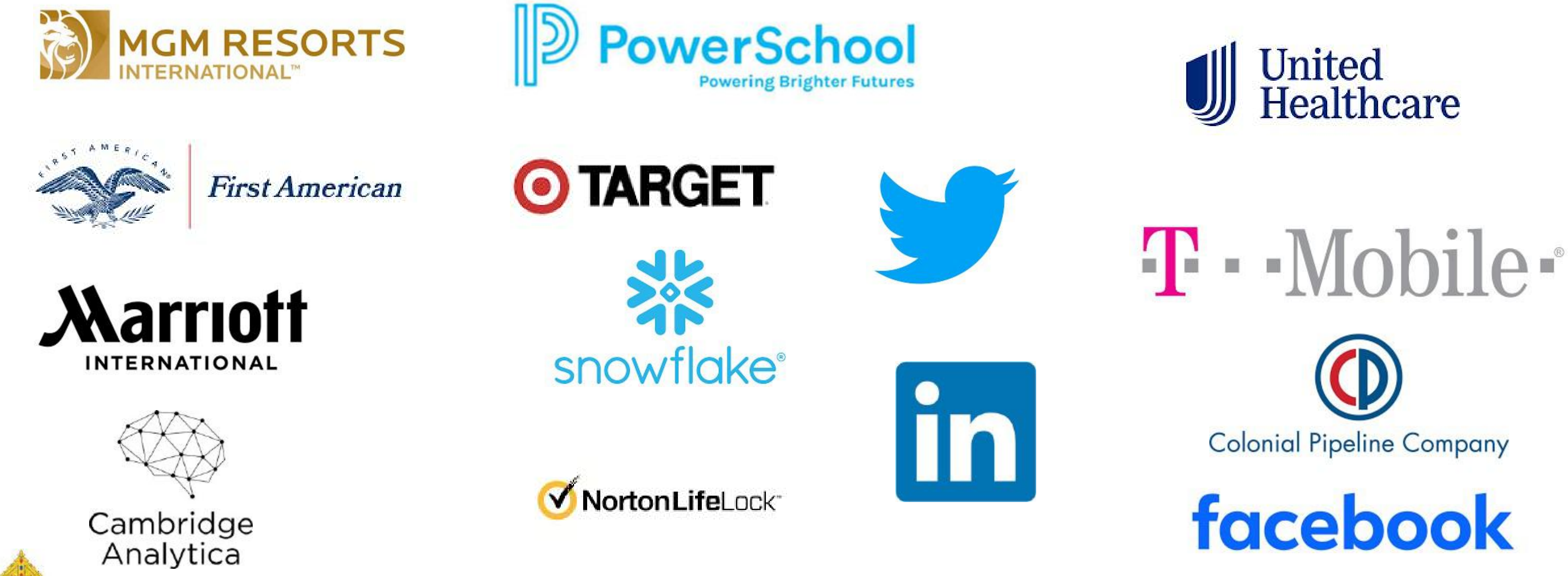
The AOS-365 Platform, an optimized version of Microsoft’s 365 infrastructure, designed to add enhanced security capabilities, adherence to Archdiocesan policies and deliver capabilities well beyond Microsoft’s M365 standard platform. Highly automated, administrative tasks such as centralized device management, backup & restore, archives and virus & malware detection continuously reduces the risk of nefarious actors penetrating your infrastructure. Professionally monitored and maintained, the AOS-365 tenant is a key component of the archdiocese’s cyber defense infrastructure.

AOS-365 Platform – Archdiocese of Seattle

Overall Benefits of a Unified Master Microsoft 365 System

- Secure – Communications and Compute within your Parish and/or School are secure and private. Threat Remediation can quickly address potential exploits across the entire ecosystem.
- Professional Support – Administrative functions are performed by industry professionals providing unparalleled support for your Parish and/or School.
- Features - Capabilities beyond the standard Microsoft M365 platform.
- Administrative Responsibilities, adding users, backup & restore, archiving and others are removed from your staff members.
- Two-Factor Authentication – To protect against stolen identities.
- Security Awareness Training – Industry Leading (KnowBe4) security awareness training for your staffs.

Threats – Current Landscape


MGM RESORTS INTERNATIONAL™
PowerSchool
Powering Brighter Futures
United Healthcare
FIRST AMERICAN
First American
TARGET
T · · Mobile ·
Marriott INTERNATIONAL
snowflake
in
Colonial Pipeline Company
Cambridge Analytica
NortonLifeLock
facebook