INFORMATION SECURITY FOUNDATIONS

PARTICIPANT GUIDE

UNITED WHOLESALE MORTGAGE

TABLE OF CONTENTS

UNITED WHOLESALE MORTGAGE

INFORMATION SECURITY FOUNDATIONS

OVERVIEW

Information Security (InfoSec) is at the heart of UWM's elite client service. If our clients (independent mortgage brokers) did not trust us with their clients' (American home buyers and owners) information, our exponential growth in the past few years would never have been possible. Being #1 is not just about mortgage sales, it is about keeping our data protected.

WARM-UP ACTIVITY:

Let's see how Information Security has already made an impact on your life. If you have an experience related to any of the questions below, write a short summary about the experience:

Have you worked somewhere that experienced a data breach?

Have you or someone you know ever had an account hacked?

Have you or someone you know ever been scammed through email or social media?

OUTCOMES

By completing this training, you will be able to:

- Identify 4 Information Security best practices for team members
- Practice recognizing common indicators of phishing attempts

UWM
UNITED WHOLESALE MORTGAGE

INFORMATION SECURITY AT UWM

Our Information Security team is divided into eight (8) main areas:

Security Operations Center (SOC): They are our "tactical swat team" located in the glass rooms by the bridge. This team is the first responder to cyber threats.

Identity and Access Management (IAM): They control the keys to the kingdom. Ensure you have correct and appropriate access to do your job correctly.

Security Engineering and Administration: This team ensures the business systems are communicating securely across the internet and systems are configured to meet UWM IT Security Standards.

Principal Engineering: This team drives continuous improvement across our UWM systems and evaluates existing systems and projects for UWM standards.

IT Governance, Risk, and Compliance (IT GRC): This team helps us maintain us navigate the Federal and State rules and provides direction to not only IT but Enterprise Technology teams as well.

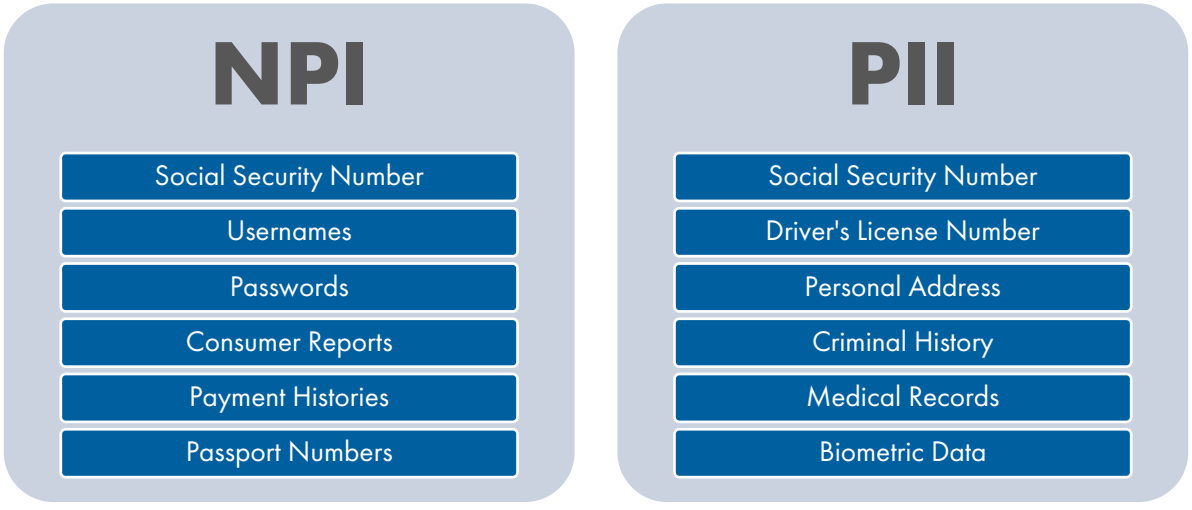
Identity Cloud and Endpoint Engineering (ICE): This team engineers identity solutions, develop works flows and automations, and protect all endpoints.

Leadership, Architecture, and Technical Delivery Manager: This team is responsible for strategy and vision, roadmaps, and aligned with other IT and business teams.

Threat and Vulnerability Management, Offensive Security: This team emulates bad guys and track vulnerabilities to completion to make sure the bad guys can't enter.

NPI VS PII

When we talk about data, there are two terms you should be aware of – Non-Public Personal Information (NPI) and Personally Identifiable Information (PII):



UNITED WHOLESALE MORTGAGE

INFORMATION SECURITY BEST PRACTICES

At UWM, there are several policies and best practices that team members use to help ensure our data is kept secure and reduce the risk of breaches. The sections below detail some of those policies and key practices.

PASSWORDS

The easiest way to be a valuable contributor to our InfoSec best practices is to create and use strong passwords. Use the pro-tips below for creating strong passwords:

- Avoid using the same password for work and personal accounts
- Basic passwords are high-risk passwords
- Use 12-16 characters (minimum), including letters, numbers, and symbols

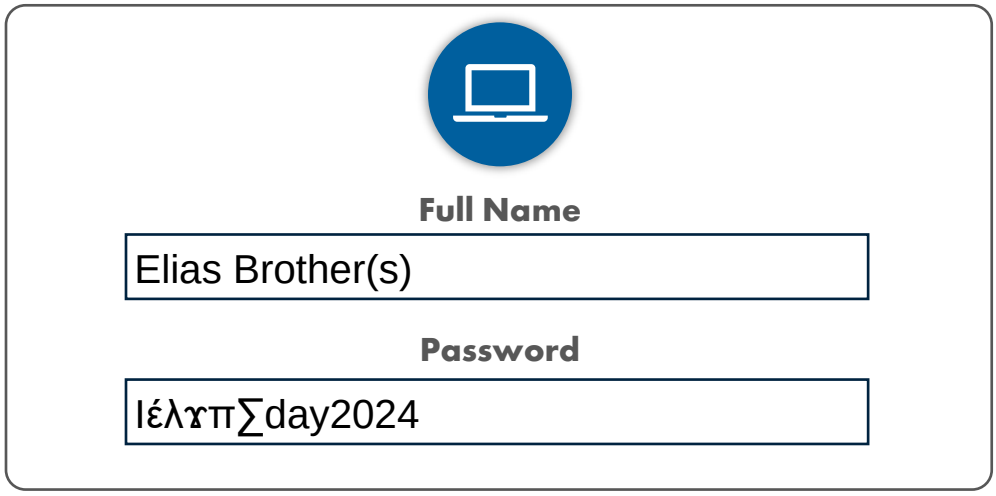
One way to build a strong password is to take a phrase you know and substitute it in alternate characters until it would be indecipherable to anyone except yourself.

For example, you might use a famous quote that means something to you, like "If you think you are too small to make a difference, try sleeping with a mosquito" and convert it into a passphrase: **iUtuR2s2maD_tSW@M!**

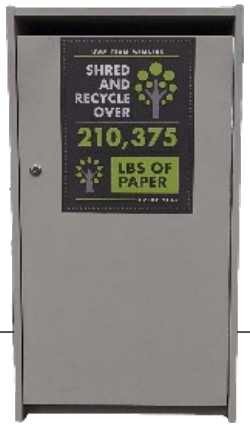
Notes:

ACTIVITY: CREATE A PASSPHRASE

Working with someone a partner, pick a famous person or character and come up with a strong passphrase.



CLEAN DESK POLICY



At the end of each day, you should make sure that all business-related paperwork is off your desk. If you need to dispose of documents that may contain sensitive information, make sure to use the shredding bins. They are most often located near the printers across our campus. Check out this infographic for keeping your desk clean and information secure.

Notes:

- Keep sensitive documents in desks / cabinets
- Maintain files on UWM's premises
- Get leadership approval before taking information off-site
- Use shredding bins around building

LOCK BEFORE YOU LEAVE POLICY

In general, it's more likely that you'll have sensitive documents (or access to sensitive documents) on your computer. It is crucial that we lock our computers when we leave them unattended. To do so, just press the power button on your dock or laptop once, or use the keyboard shortcut Windows + L.

If you do accidentally leave your computer unlocked while you're away from your desk, an Information Security team member may take corrective action, as this is a significant security concern. If your computer is found unlocked by an Information Security team member, they will lock your computer, change your background to the image below, and make a record of this occurrence.

USB AND EXTERNAL STORAGE DEVICE POLICY

Because we work with sensitive information daily, the usage of USB and external storage devices is not allowed.

Notes:

ACTIVITY: CLEAN DESK ADVICE

Following the guidance of your trainer, observe two photos of team members desks on the screen. Using the space below, write your advice to the team member to help them comply with the clean desk policy:

DESK 1:

- Computer not locked
- PII information exposed / left open on desk
- PII information left displayed on computer monitors and laptop screen
- Password in plain text, on sticky-note, attached to monitor, in the open for all to see

DESK 2:

- Computer not locked
- Keys for sensitive location available on desk
- USB drives on desk / available to someone else
- PII on notepad left open on desk
- PII left up on computer screen

REFLECTION: INFORMATION SECURITY BEST PRACTICES

Use the space below to write any areas of opportunity you may have when it comes to implementing these best practices. Can you work on stronger passwords? Can you work on keeping sensitive documents in filing cabinets? Sound off below:

PHISHING

Phishing is a fraudulent attempt to obtain sensitive information or data, such as usernames, passwords, credit card details, and other sensitive details. 91% of attacks start with email.

Notes:

MIMECAST

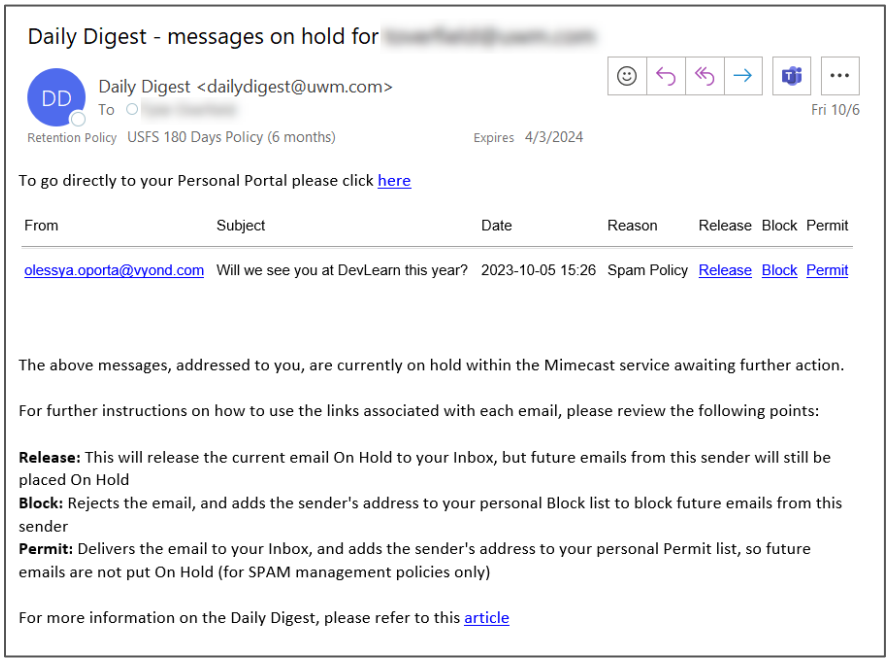
Mimecast is a cloud cybersecurity tool used for scanning incoming emails to check for possible signs of malicious content or just spam.

MIMECAST DAILY DIGEST EMAIL

When Mimecast® puts email on hold, you will get an email called the Daily Digest. This email will show you what messages have been put on hold and will allow you to manage them from the Daily Digest.

You can do the following with these on-hold emails:

- **Release** – This allows the email to come to your inbox.
- **Block** – This blocks the email and all future emails from this sender.
- **Permit** – This allows the email and all future emails from this sender.



Daily Digest - messages on hold for [redacted]

DD Daily Digest <dailydigest@uwm.com>
To [redacted]
Fri 10/6

Retention Policy USFS 180 Days Policy (6 months) Expires 4/3/2024

To go directly to your Personal Portal please click here

From	Subject	Date	Reason	Release	Block	Permit
olessya.oporta@vyond.com	Will we see you at DevLearn this year?	2023-10-05 15:26	Spam Policy	Release	Block	Permit

The above messages, addressed to you, are currently on hold within the Mimecast service awaiting further action.

For further instructions on how to use the links associated with each email, please review the following points:

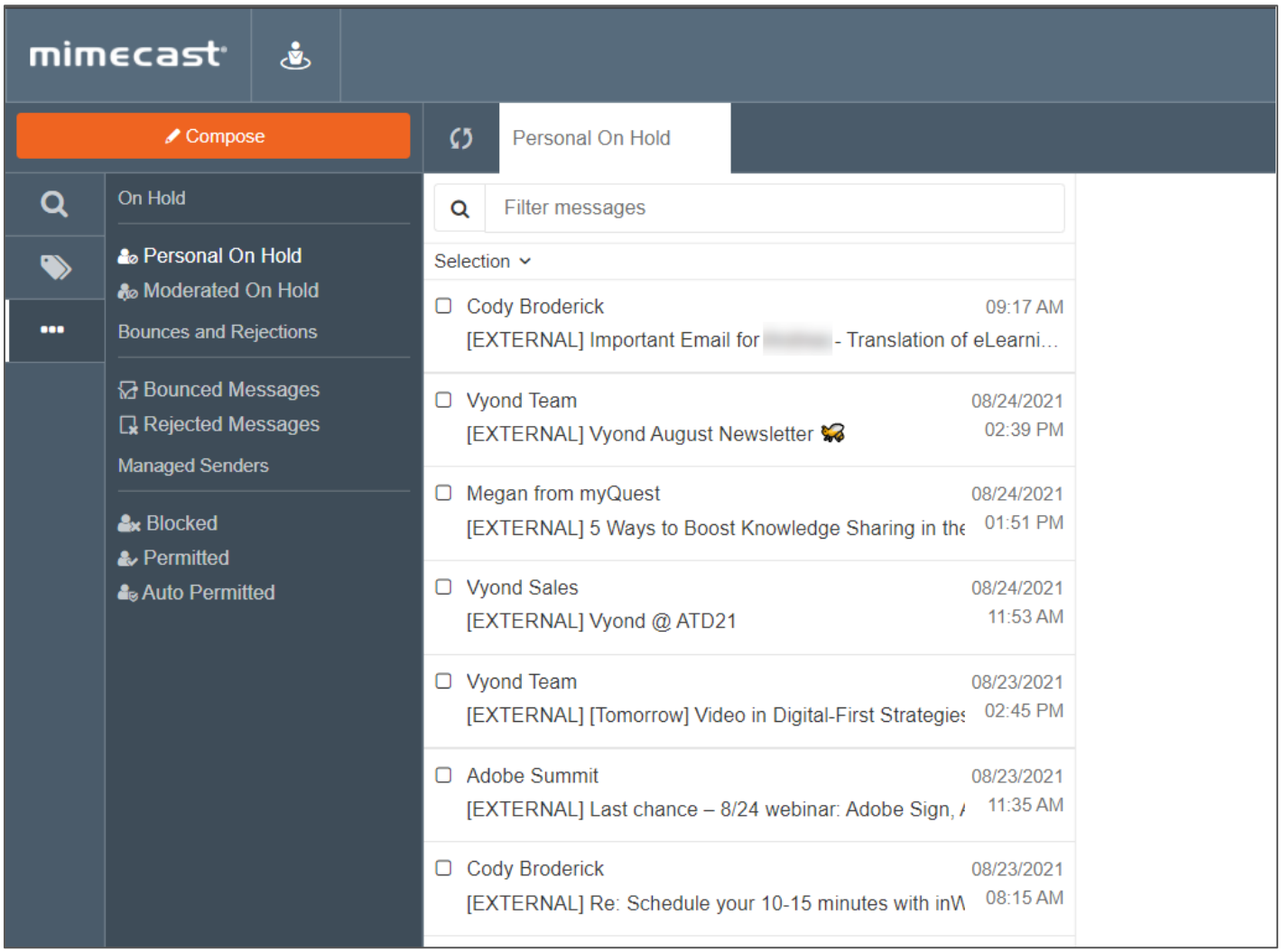
Release: This will release the current email On Hold to your Inbox, but future emails from this sender will still be placed On Hold
Block: Rejects the email, and adds the sender's address to your personal Block list to block future emails from this sender
Permit: Delivers the email to your Inbox, and adds the sender's address to your personal Permit list, so future emails are not put On Hold (for SPAM management policies only)

For more information on the Daily Digest, please refer to this article

MIMECAST PERSONAL PORTAL

Along with the Daily Digest email, you can also use your Personal Portal in Mimecast® to manage your on-hold emails. To access your portal, you can:

1) Use the link at the top of the Daily Digest email, or link in the Launcher of UZone.
2) Navigate to Mimecast Login[1] and login with SSO.



COMMON PHISHING EMAIL INDICATORS

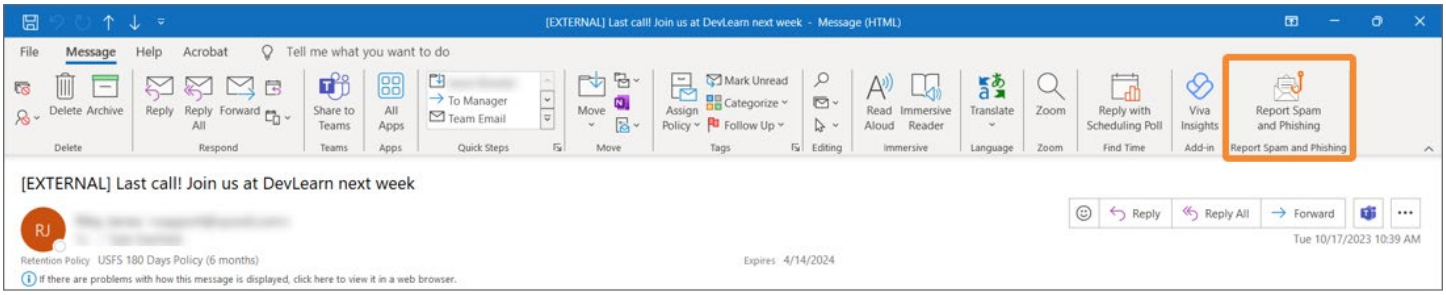
Cybercriminals are improving their tactics on getting you to give valuable information. With tools like Mimecast®, our IT Team helps us reduce the number that make it to your inbox, but some will still get through! Phishing attempts are getting harder to recognize, but there are a few common indicators to look for when interacting with any messages.

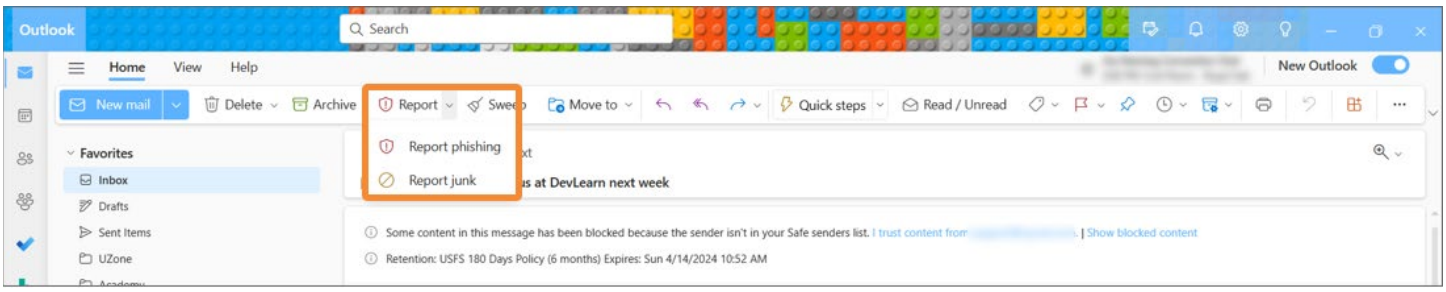
Take notes below as we review common indicators together. You can also find an infographic in Academy that highlights common red flags.

Notes:

REPORT SPAM AND PHISHING

If you discover a suspicious email in your inbox, do not click any attached links or documents. Merely clicking these often grants hackers access to our systems, from which they can access huge swaths of data or enact locks on our systems and demand a ransom fee. Instead, click the **Report Spam & Phishing** button in Outlook, marked below:





UNITED WHOLESALE MORTGAGE

ACTIVITY: GOOGLE PHISH PRONE

Let's take a quiz designed by Google to help troubleshoot our current skill level in detecting phishing attempts!

Click on the following link and take the quiz: phishing quiz.withgoogle.com[2]. Afterward, we'll discuss our results as a class.

What was your score? What tricked you in any of the practice emails?

7 / 8. The "TripIt" service wanted to scan my email.

FINAL TAKEAWAY

Use the space below to write any final takeaways on Information Security:

ADDITIONAL RESOURCES

Phishing Infographic[3]

- This infographic highlights common red flags that an email may be a phishing attempt.

Clean Desk Infographic[4]

- Some tips for keeping your desk clean and information secure.

HYPERLINKS IN THIS DOCUMENT

1. https://login.mimecast.com/u/login/?gta=apps#/login
2. https://phishingquiz.withgoogle.com/
3. https://uwm.csod.com/ui/lms-learning-details/app/material/4c420610-79b9-4257-8ba5-f109841a1157
4. https://uwm.csod.com/clientimg/uwm/MaterialSource/d80eed2e-f481-4ef5-b041-d2f4fe7ddd62_Lock_or_Leave__Infographic_v1_FINAL.pdf

If you have any questions or concerns, please reach out to the Information Security team at InfoSec@uwm.com.