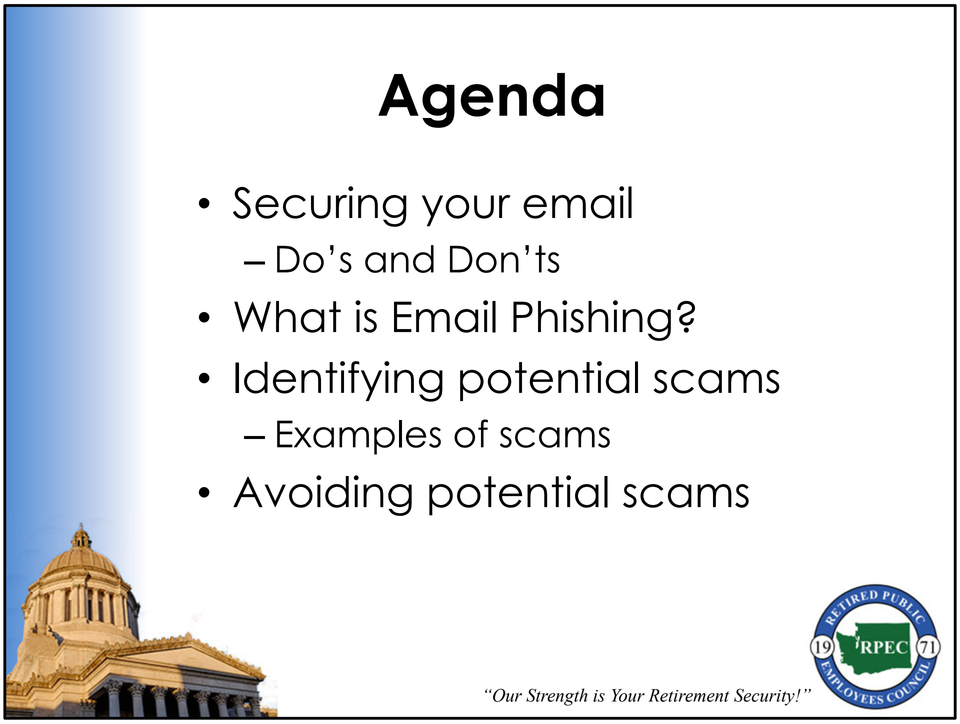
Protecting Your Email & Avoiding Online Scams

"Our Strength is Your Retirement Security!"

Welcome!



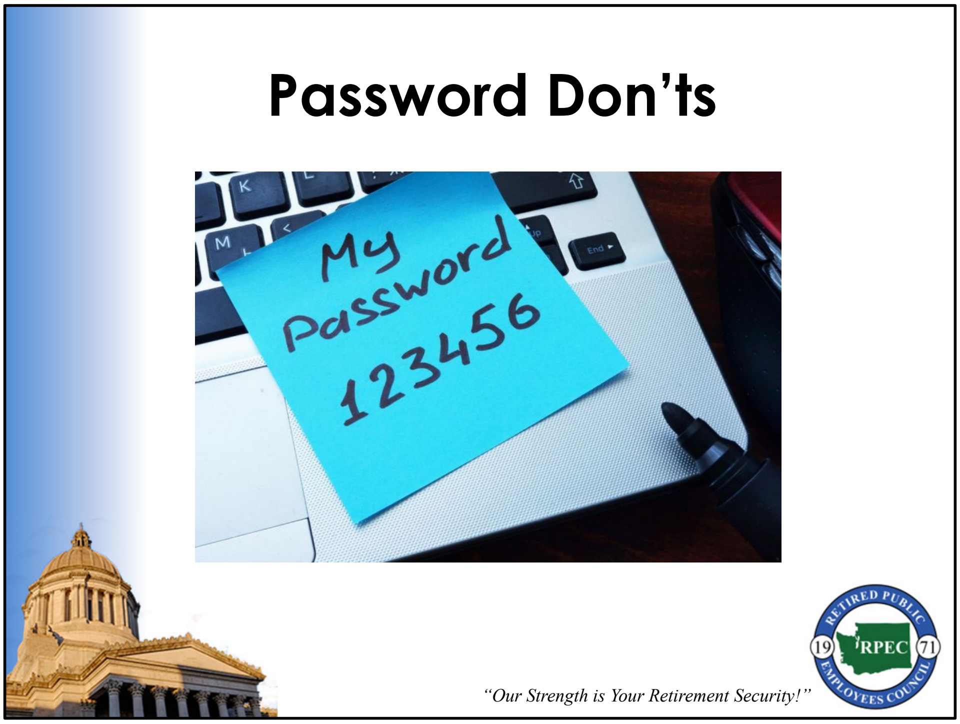
Agenda

- Securing your email
  - Do's and Don'ts
- What is Email Phishing?
- Identifying potential scams
  - Examples of scams
- Avoiding potential scams

"Our Strength is Your Retirement Security!"

Agenda

1. Securing your email – we are going to go over best practice ways of keeping your email secure at a basic user level.
2. What is email phishing? – we will go over types of email phishing scams and what kind of information scammers are after.
3. Identifying potential scams – we will be teaching you some simple methods to help you to better identify potential scams and what to look.
4. Avoiding potential scams – ways to avoid spam and reduce the amount you may receive.

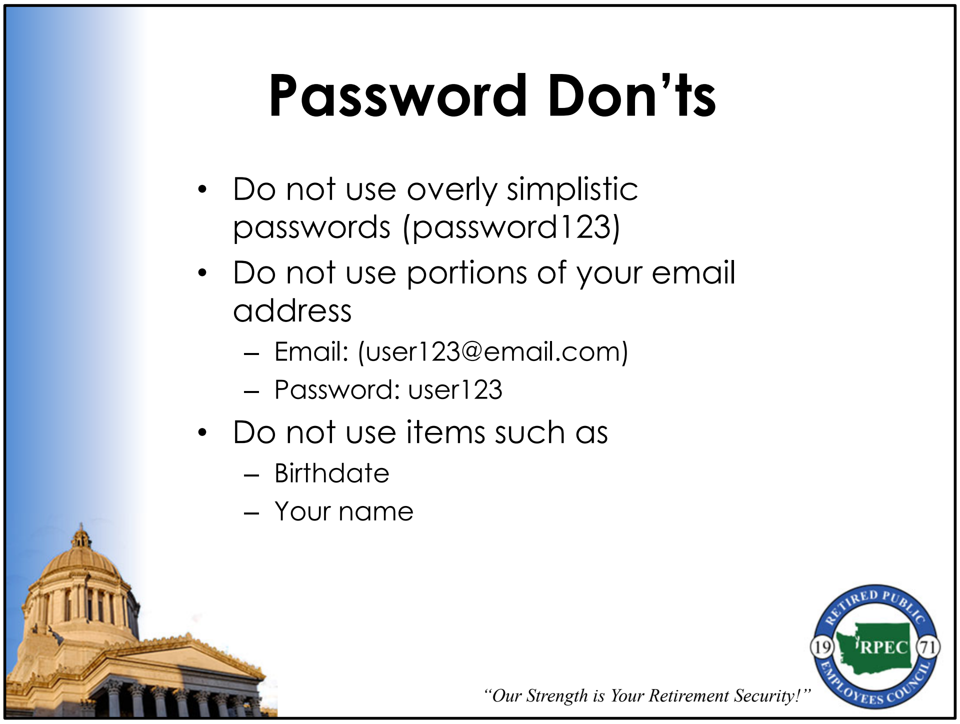


Password Don’ts

“Our Strength is Your Retirement Security!”

Do not use simplistic passwords like:

- 123456abc123
- password
- password1
- password123



Password Don’ts

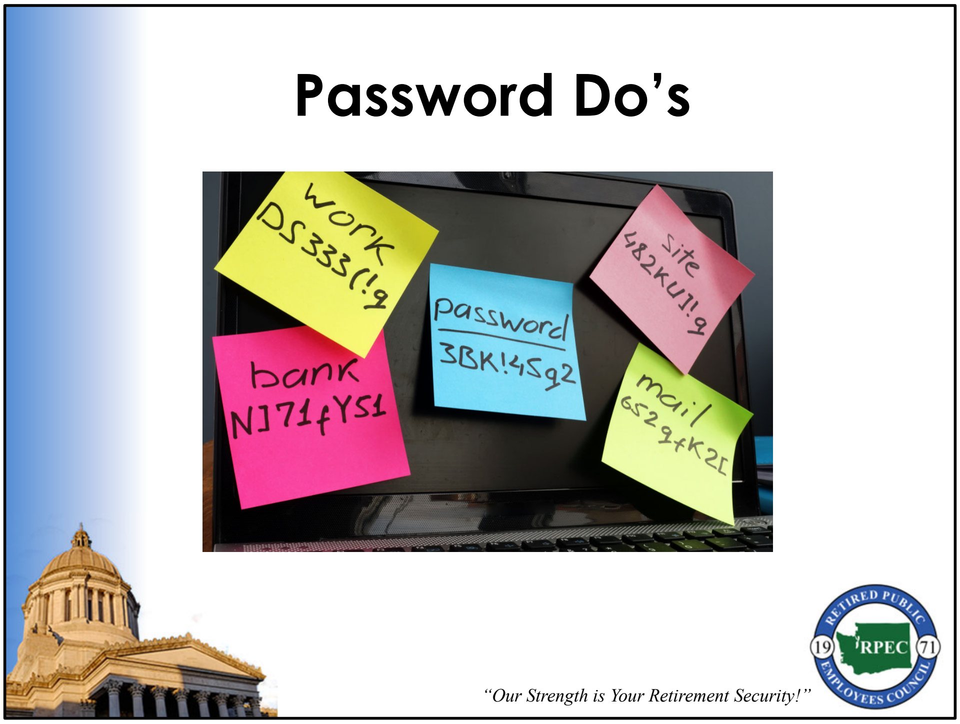
- Do not use overly simplistic passwords (password123)
- Do not use portions of your email address
  - Email: (user123@email.com)
  - Password: user123
- Do not use items such as
  - Birthdate
  - Your name

“Our Strength is Your Retirement Security!”

RETIRED PUBLIC EMPLOYEES COUNCIL
19
RPEC
71

Do not use simplistic passwords like:

- Password that are same as username.
- Personal information as password (name, city, birthday, family member names)

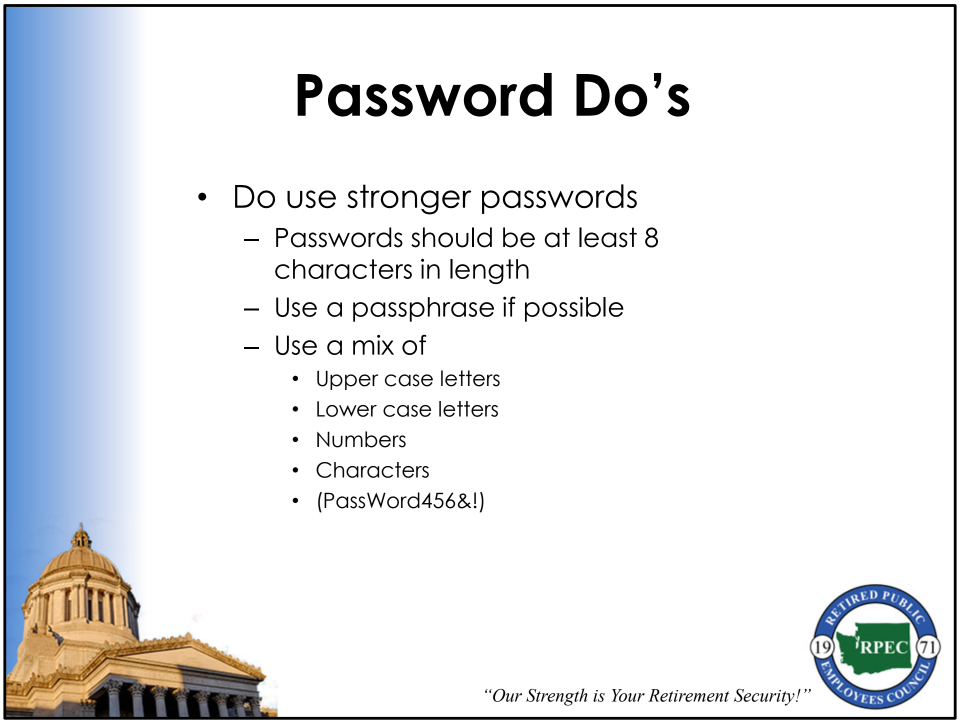


Password Do’s

“Our Strength is Your Retirement Security!”

A strong password is:

- At least 12 characters long but 14 or more is better.
- A combination of uppercase letters, lowercase letters, numbers, and symbols.



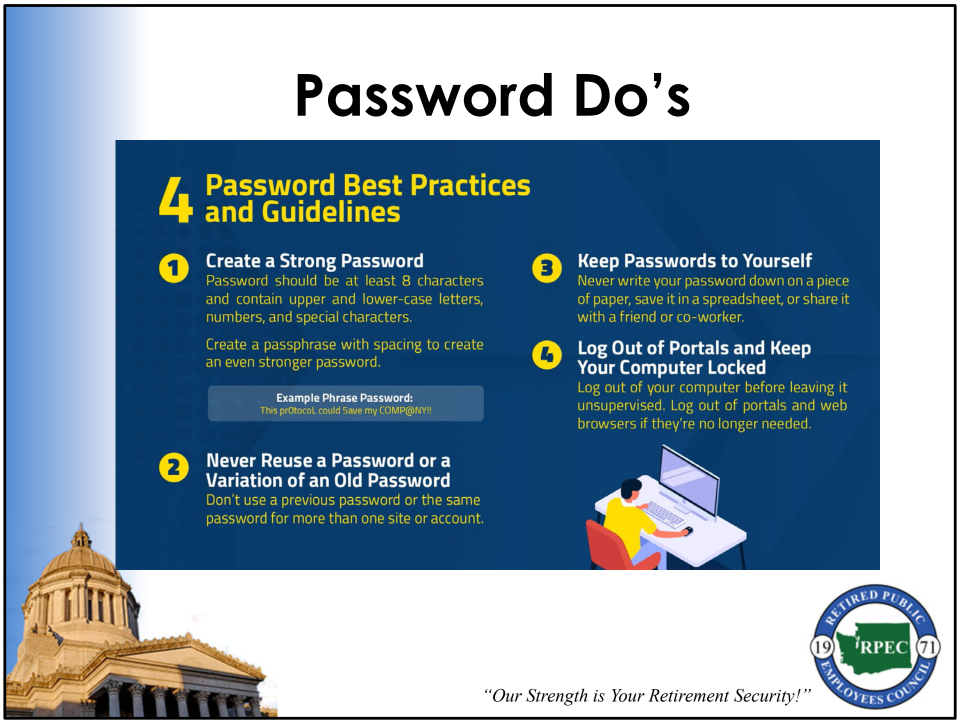
Password Do’s

- Do use stronger passwords
  - Passwords should be at least 8 characters in length
  - Use a passphrase if possible
  - Use a mix of
    - Upper case letters
    - Lower case letters
    - Numbers
    - Characters
    - (PassWord456&!)

RETIRED PUBLIC EMPLOYEES COUNCIL
19
RPEC
71

“Our Strength is Your Retirement Security!”

- Rule 1: use at least 8 characters. ...
- Rule 2: use combination of different characters. ...
- Rule 3: use at least one uppercase. ...
- Rule 4: never use common information in your password. ...
- Rule 5: never use the same password twice. ...



Password Do's

4 Password Best Practices and Guidelines

1 Create a Strong Password
Password should be at least 8 characters and contain upper and lower-case letters, numbers, and special characters.

Create a passphrase with spacing to create an even stronger password.

Example Phrase Password:
This pr0tocoL could 5ave my COMP@NY!!

2 Never Reuse a Password or a Variation of an Old Password
Don't use a previous password or the same password for more than one site or account.

3 Keep Passwords to Yourself
Never write your password down on a piece of paper, save it in a spreadsheet, or share it with a friend or co-worker.

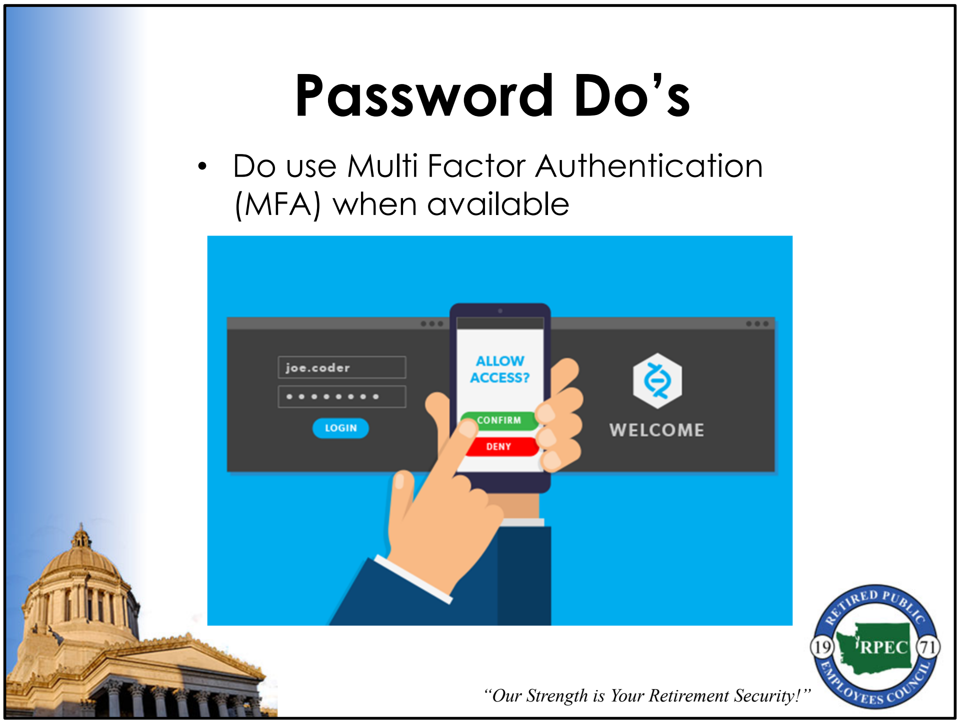
4 Log Out of Portals and Keep Your Computer Locked
Log out of your computer before leaving it unsupervised. Log out of portals and web browsers if they're no longer needed.

RETIRED PUBLIC EMPLOYEES COUNCIL 19 RPEC 71

"Our Strength is Your Retirement Security!"

Do:

1. Create a strong password
2. Never re-use an old password or a variation of it.
3. Keep passwords to yourself.
4. Log out and lock your computer.



Password Do's

- Do use Multi Factor Authentication (MFA) when available

"Our Strength is Your Retirement Security!"

Do use Multi Factor Authentication when available

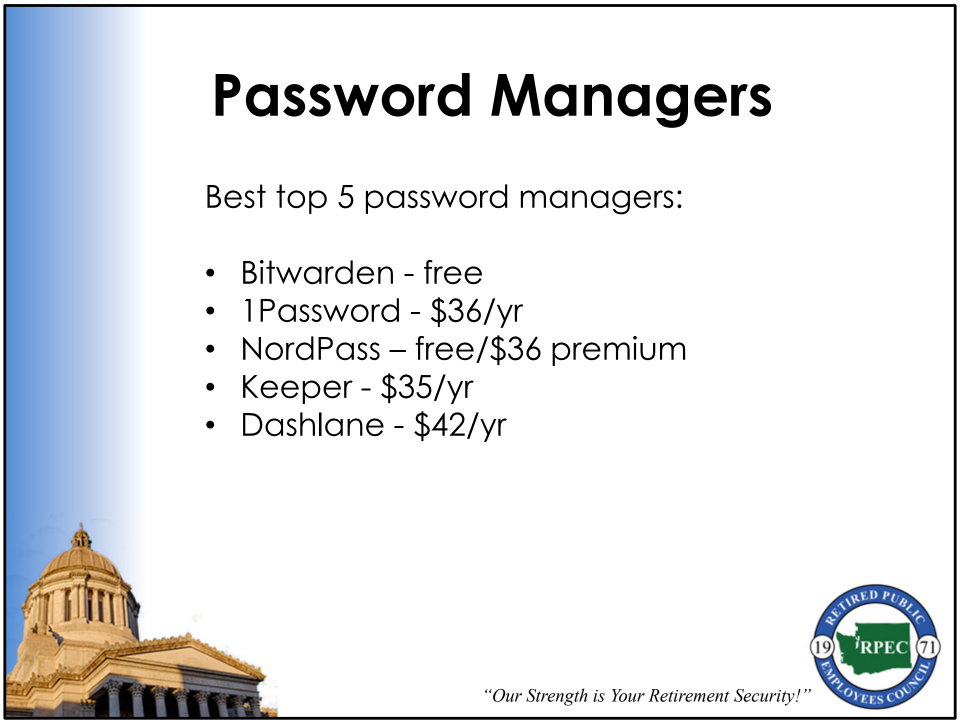
Password Managers

"Our Strength is Your Retirement Security!"

Password Managers are an application, either residing on your computer, as part of your browser, or online that you store company and personal websites and their associated login information in.

A password manager is a tool that does the work of creating, remembering and filling in passwords.

A password manager is a software application designed to store and manage online credentials. Usually, these passwords are stored in an encrypted database and locked behind a master password.



Password Managers

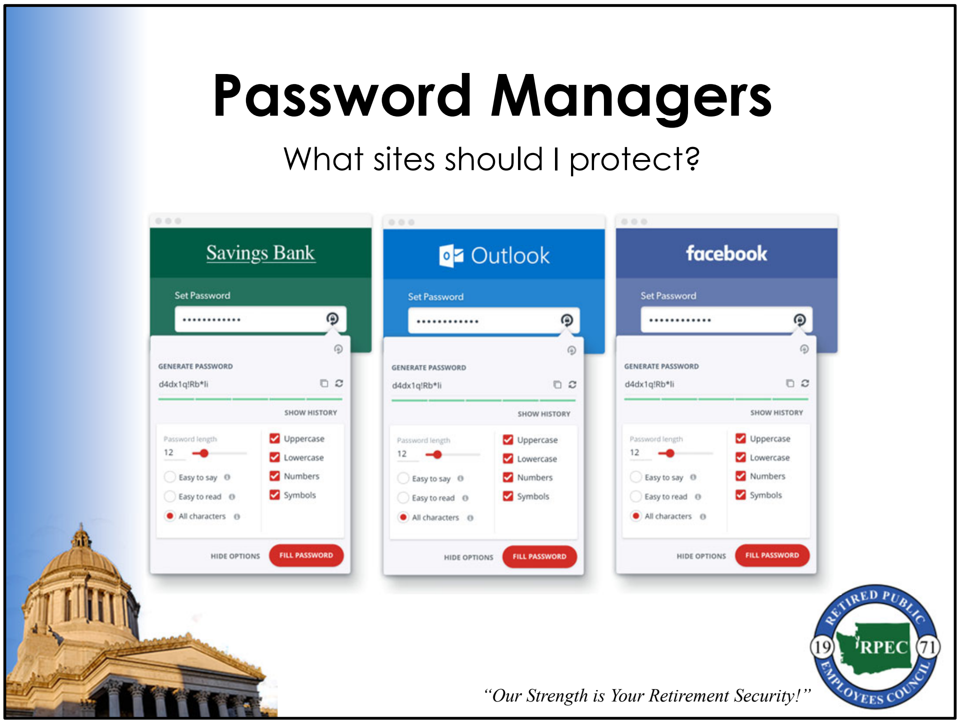
Best top 5 password managers:

- Bitwarden - free
- 1Password - $36/yr
- NordPass – free/$36 premium
- Keeper - $35/yr
- Dashlane - $42/yr

"Our Strength is Your Retirement Security!"

Best top 5 password managers:

Bitwarden - free
1Password - $36/yr
NordPass – free/$36 premium
Keeper - $35/yr
Dashlane - $42/yr



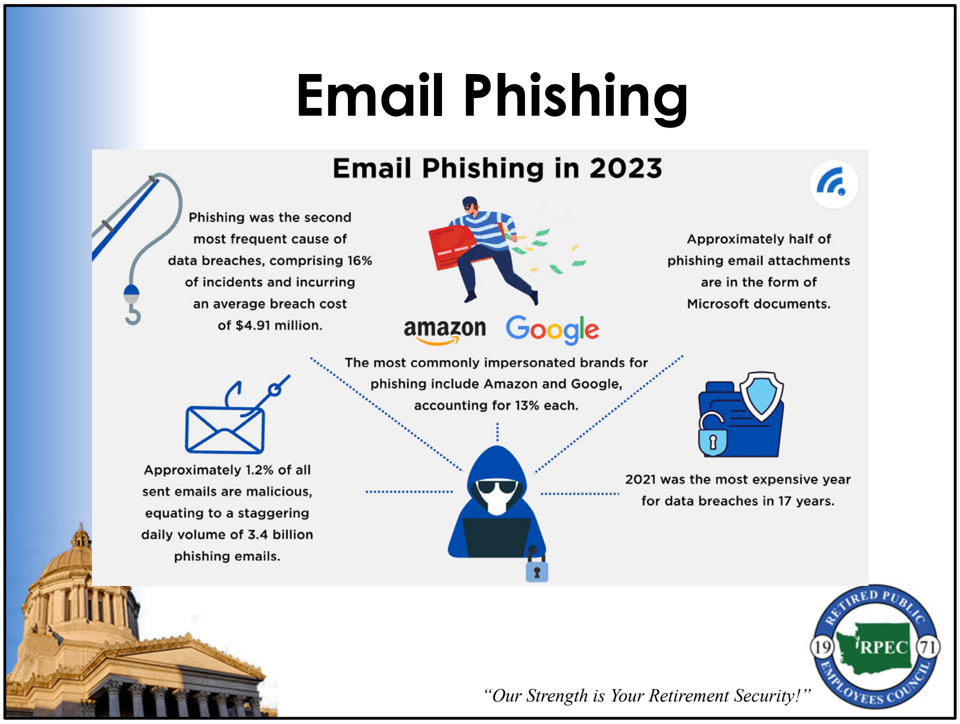
Password Managers

What sites should I protect?

"Our Strength is Your Retirement Security!"

What sites should I protect?

- Banking
- Email
- Services – Amazon, Netflix, Stores
- Social Media accounts



Email Phishing

Email Phishing in 2023

Phishing was the second most frequent cause of data breaches, comprising 16% of incidents and incurring an average breach cost of $4.91 million.

The most commonly impersonated brands for phishing include Amazon and Google, accounting for 13% each.

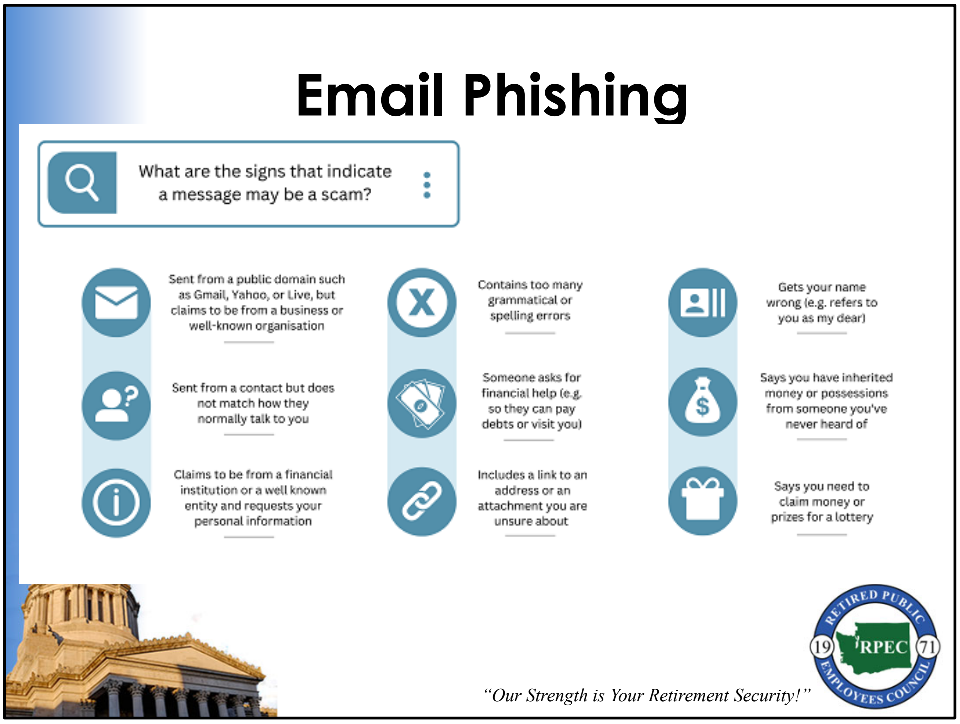
Approximately half of phishing email attachments are in the form of Microsoft documents.

Approximately 1.2% of all sent emails are malicious, equating to a staggering daily volume of 3.4 billion phishing emails.

2021 was the most expensive year for data breaches in 17 years.

"Our Strength is Your Retirement Security!"

Email phishing statistics for 2023



Email Phishing

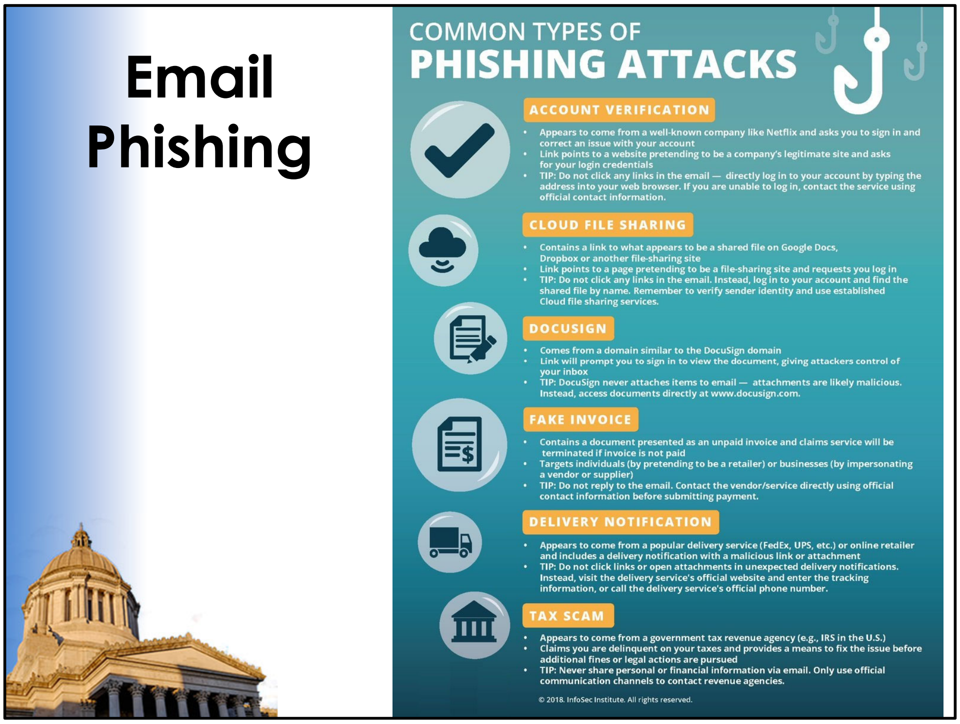
What are the signs that indicate a message may be a scam?

- Sent from a public domain such as Gmail, Yahoo, or Live, but claims to be from a business or well-known organisation
- Sent from a contact but does not match how they normally talk to you
- Claims to be from a financial institution or a well known entity and requests your personal information
- Contains too many grammatical or spelling errors
- Someone asks for financial help (e.g. so they can pay debts or visit you)
- Includes a link to an address or an attachment you are unsure about
- Gets your name wrong (e.g. refers to you as my dear)
- Says you have inherited money or possessions from someone you've never heard of
- Says you need to claim money or prizes for a lottery

"Our Strength is Your Retirement Security!"

What are the signs that a message may be a scam?

- Claims to be from a company/business but the sender's address is from a domain such as Gmail, Yahoo, or from an unrecognizable domain or foreign domain.
- From a contact or yours, but worded not the way they normally speak.
- Grammatical or spelling errors.
- Requests you to log in thru a link in the email.



Email Phishing

COMMON TYPES OF PHISHING ATTACKS

ACCOUNT VERIFICATION

- Appears to come from a well-known company like Netflix and asks you to sign in and correct an issue with your account
- Link points to a website pretending to be a company's legitimate site and asks for your login credentials
- TIP: Do not click any links in the email — directly log in to your account by typing the address into your web browser. If you are unable to log in, contact the service using official contact information.

CLOUD FILE SHARING

- Contains a link to what appears to be a shared file on Google Docs, Dropbox or another file-sharing site
- Link points to a page pretending to be a file-sharing site and requests you log in
- TIP: Do not click any links in the email. Instead, log in to your account and find the shared file by name. Remember to verify sender identity and use established Cloud file sharing services.

DOCUSIGN

- Comes from a domain similar to the DocuSign domain
- Link will prompt you to sign in to view the document, giving attackers control of your inbox
- TIP: DocuSign never attaches items to email — attachments are likely malicious. Instead, access documents directly at www.docusign.com.

FAKE INVOICE

- Contains a document presented as an unpaid invoice and claims service will be terminated if invoice is not paid
- Targets individuals (by pretending to be a retailer) or businesses (by impersonating a vendor or supplier)
- TIP: Do not reply to the email. Contact the vendor/service directly using official contact information before submitting payment.

DELIVERY NOTIFICATION

- Appears to come from a popular delivery service (FedEx, UPS, etc.) or online retailer and includes a delivery notification with a malicious link or attachment
- TIP: Do not click links or open attachments in unexpected delivery notifications. Instead, visit the delivery service's official website and enter the tracking information, or call the delivery service's official phone number.

TAX SCAM

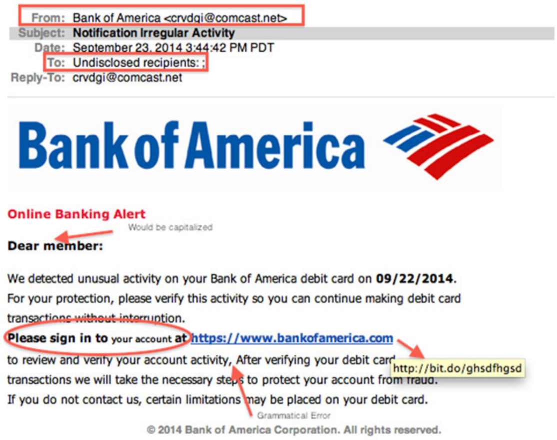
- Appears to come from a government tax revenue agency (e.g., IRS in the U.S.)
- Claims you are delinquent on your taxes and provides a means to fix the issue before additional fines or legal actions are pursued
- TIP: Never share personal or financial information via email. Only use official communication channels to contact revenue agencies.

Common Types of Attacks

Account Verification
Fake Invoice
Delivery Notification

Never click on an attachment or link in an email you do not recognize or trust!

Identifying Email Scams



From: Bank of America <crvdgi@comcast.net>
Subject: **Notification Irregular Activity**
Date: September 23, 2014 3:44:42 PM PDT
To: Undisclosed recipients: ;
Reply-To: crvdgi@comcast.net

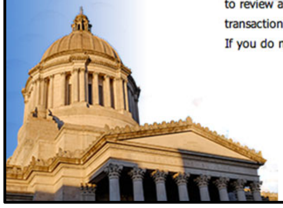
Bank of America

Online Banking Alert

Dear member:

We detected unusual activity on your Bank of America debit card on **09/22/2014**.
For your protection, please verify this activity so you can continue making debit card transactions without interruption.
Please sign in to your account **at** https://www.bankofamerica.com
to review and verify your account activity, After verifying your debit card transactions we will take the necessary steps to protect your account from fraud.
If you do not contact us, certain limitations may be placed on your debit card.

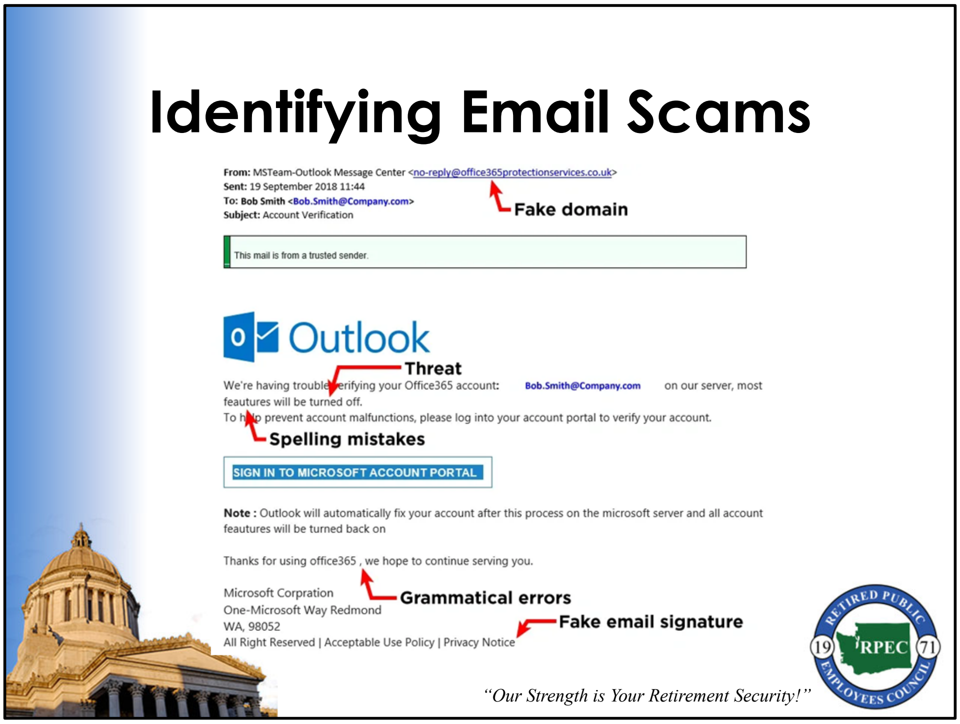
© 2014 Bank of America Corporation. All rights reserved.



"Our Strength is Your Retirement Security!"

Ways to identify spam emails:

- Email is not from actual company/business – view the email address of the sender.
- Email is often sent to an undisclosed group
- When hovering over links in the email, the URL's are not those of the legisitmate company/business.



Identifying Email Scams

From: MSTeam-Outlook Message Center <no-reply@office365protectionservices.co.uk>
Sent: 19 September 2018 11:44
To: Bob Smith <Bob.Smith@Company.com>
Subject: Account Verification

Fake domain

This mail is from a trusted sender.

Outlook

Threat

We're having trouble verifying your Office365 account: Bob.Smith@Company.com on our server, most feautures will be turned off.
To help prevent account malfunctions, please log into your account portal to verify your account.

Spelling mistakes

SIGN IN TO MICROSOFT ACCOUNT PORTAL

Note : Outlook will automatically fix your account after this process on the microsoft server and all account feautures will be turned back on

Thanks for using office365 , we hope to continue serving you.

Grammatical errors

Microsoft Corpration
One-Microsoft Way Redmond
WA, 98052
All Right Reserved | Acceptable Use Policy | Privacy Notice

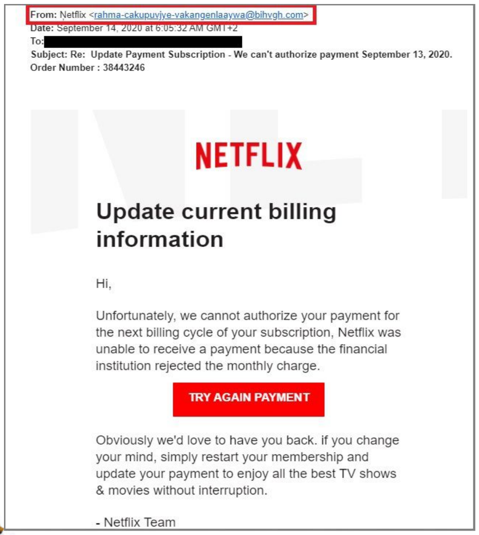
Fake email signature

"Our Strength is Your Retirement Security!"

Ways to identify spam emails:

- Email is not from actual company/business – view the email address of the sender.
- Email often conveys a threat to your account – it may close, payment didn't process, an expensive charge occurred.
- Common mistakes are found – spelling, grammar, punctuation.

Identifying Email Scams



From: Netflix <rahma-cakupuvjye-vakangenlaaywa@bihvgh.com>
Date: September 14, 2020 at 6:05:32 AM GMT+2
To: [redacted]
Subject: Re: Update Payment Subscription - We can't authorize payment September 13, 2020.
Order Number : 38443246

NETFLIX

Update current billing information

Hi,

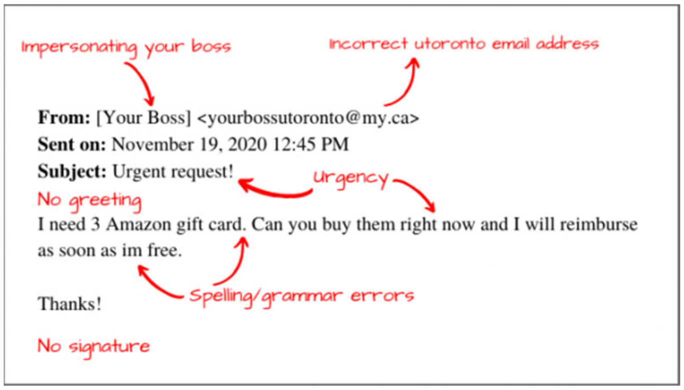
Unfortunately, we cannot authorize your payment for the next billing cycle of your subscription, Netflix was unable to receive a payment because the financial institution rejected the monthly charge.

Obviously we'd love to have you back. if you change your mind, simply restart your membership and update your payment to enjoy all the best TV shows & movies without interruption.

- Netflix Team

"Our Strength is Your Retirement Security!"

Identifying Email Scams



From: [Your Boss] <yourbossutoronto@my.ca>
Sent on: November 19, 2020 12:45 PM
Subject: Urgent request!

I need 3 Amazon gift card. Can you buy them right now and I will reimburse as soon as im free.

Thanks!

"Our Strength is Your Retirement Security!"

If unsure, STOP for a minute and Google for relevant spam emails, you will likely find a match.

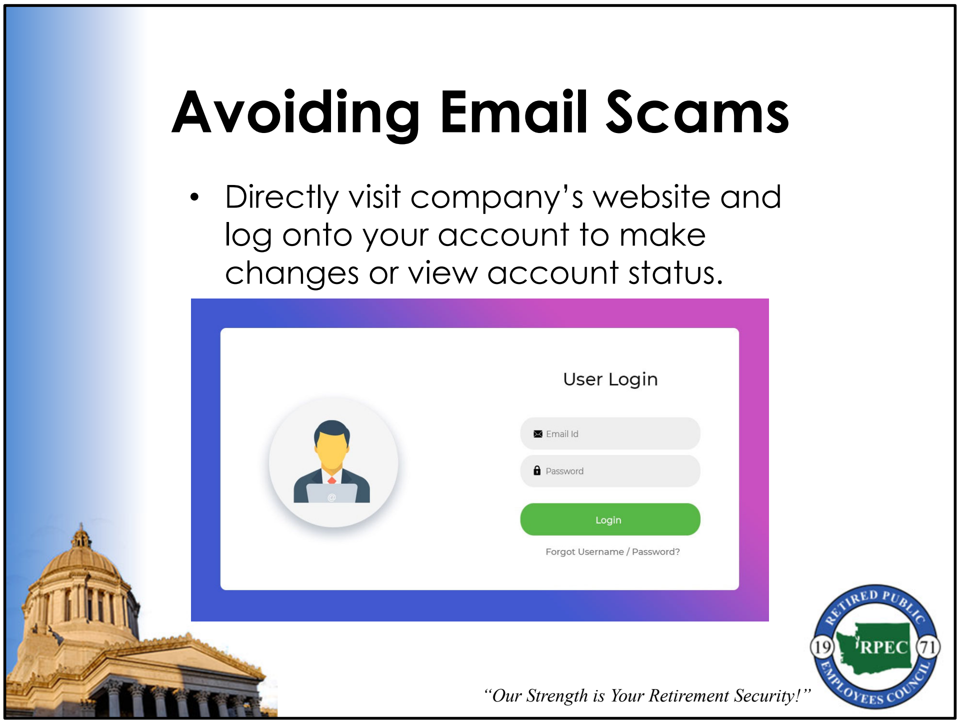
Avoiding Email Scams

- If unsure, NEVER click on a link or attachment in an email.

Be careful
what you click.

"Our Strength is Your Retirement Security!"

NEVER click a link in an email if you are unsure if message is spam or not, or if you do not know the sender.

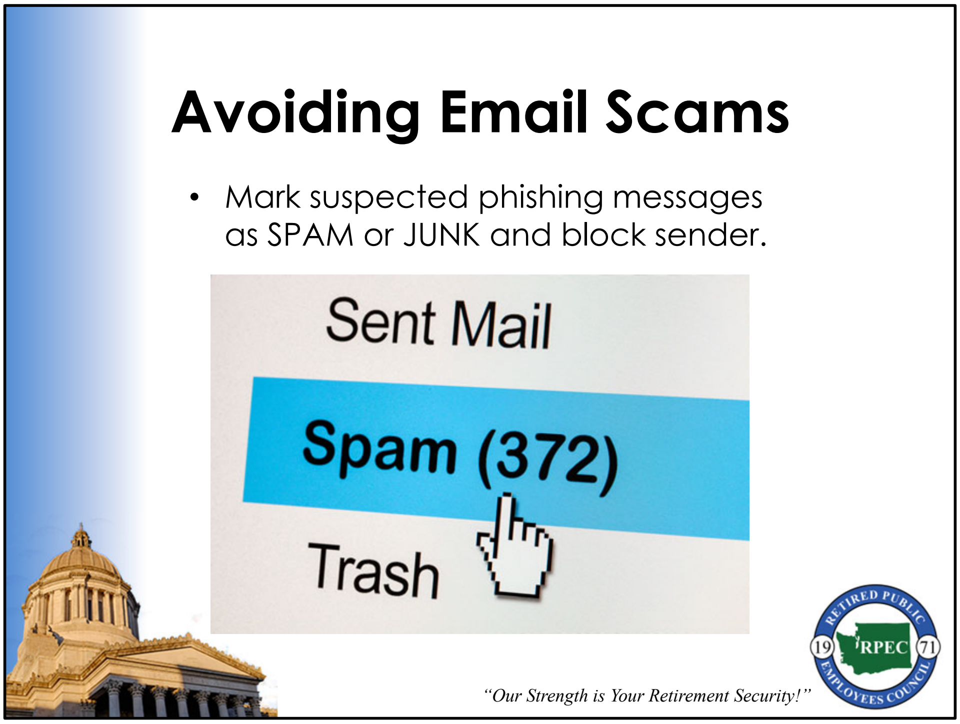


Avoiding Email Scams

- Directly visit company’s website and log onto your account to make changes or view account status.

“Our Strength is Your Retirement Security!”

If you are concerned about a potential threat to an account via email, always visit the company’s website and log on to your account to view the status, or call Customer Service through the company’s published phone number.



Avoiding Email Scams

- Mark suspected phishing messages as SPAM or JUNK and block sender.

Sent Mail
Spam (372)
Trash
RETIRED PUBLIC EMPLOYEES COUNCIL
19 RPEC 71

"Our Strength is Your Retirement Security!"

Research how to mark these messages as SPAM or JUNK, and even better yet, BLOCK SENDER.

Your email provider should have easy instructions on how to do this, either through their application or by means of a Google search.

You can also mark emails as 'friendly' by TRUST SENDER or adding the sender to your address list, like yours truly! Again, your email provider should have easy instructions on how to do this, either through their application or by means of a Google search.

Happy Emailing!

"Our Strength is Your Retirement Security!"

By implementing these simple tips, your risk of being defrauded, hacked or worse can be greatly reduced or even eliminated.

However, you must stay vigilant as the scammers are always trying to find new methods to deceive you.

Happy emailing!