Email Security and Best Practices

REV. JULY 15, 2024

How does my computer get infected?

Clicking on malicious links in emails

Plugging in an unknown flash drive

Downloading malware masquerading as other software

Phishing?
Or fishing?

- Is the act of setting the bait (trap)…
- Casting it out into a wide ocean…
- Hoping that something bites that you can then hook
- Intentionally deceiving someone by posing as a legitimate company
- Typically, utilizes email by pretending to be a company or service requesting you to do something
- Hoping that you click the link and fill out the requested info

Phishing Stats

30% of people

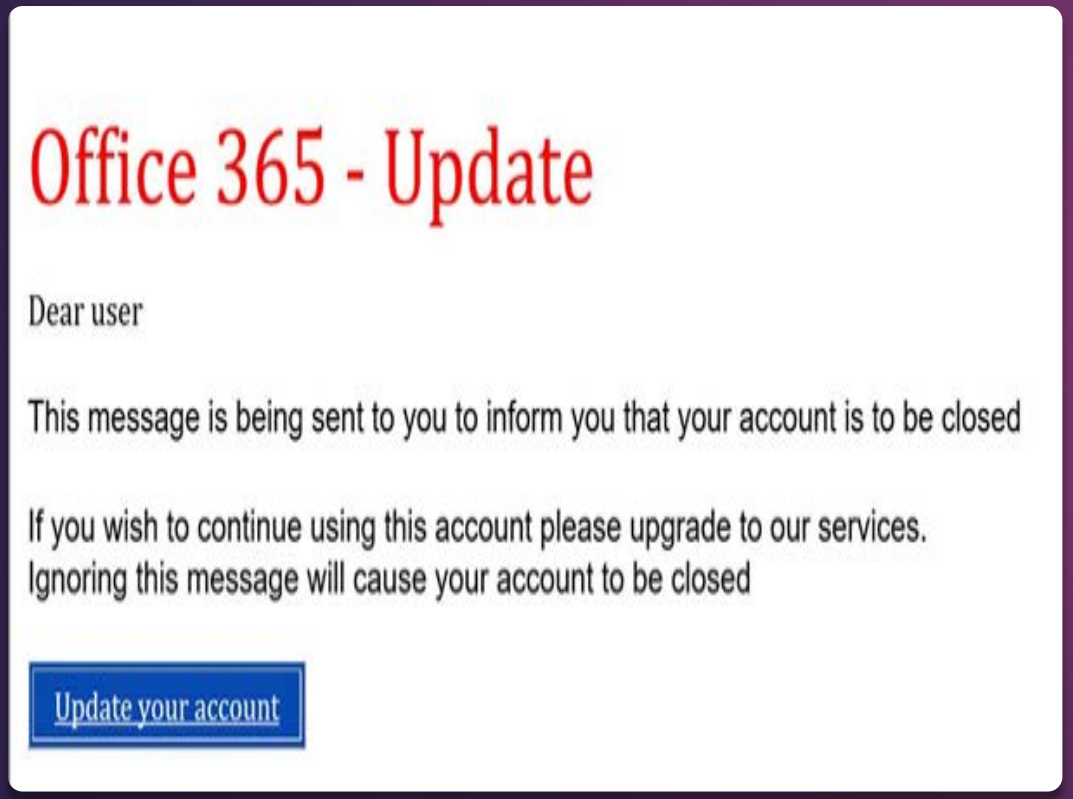
Open phishing messages
(23% last year)

12% of

people

Open attachments
(11% last year)

Phishing Examples



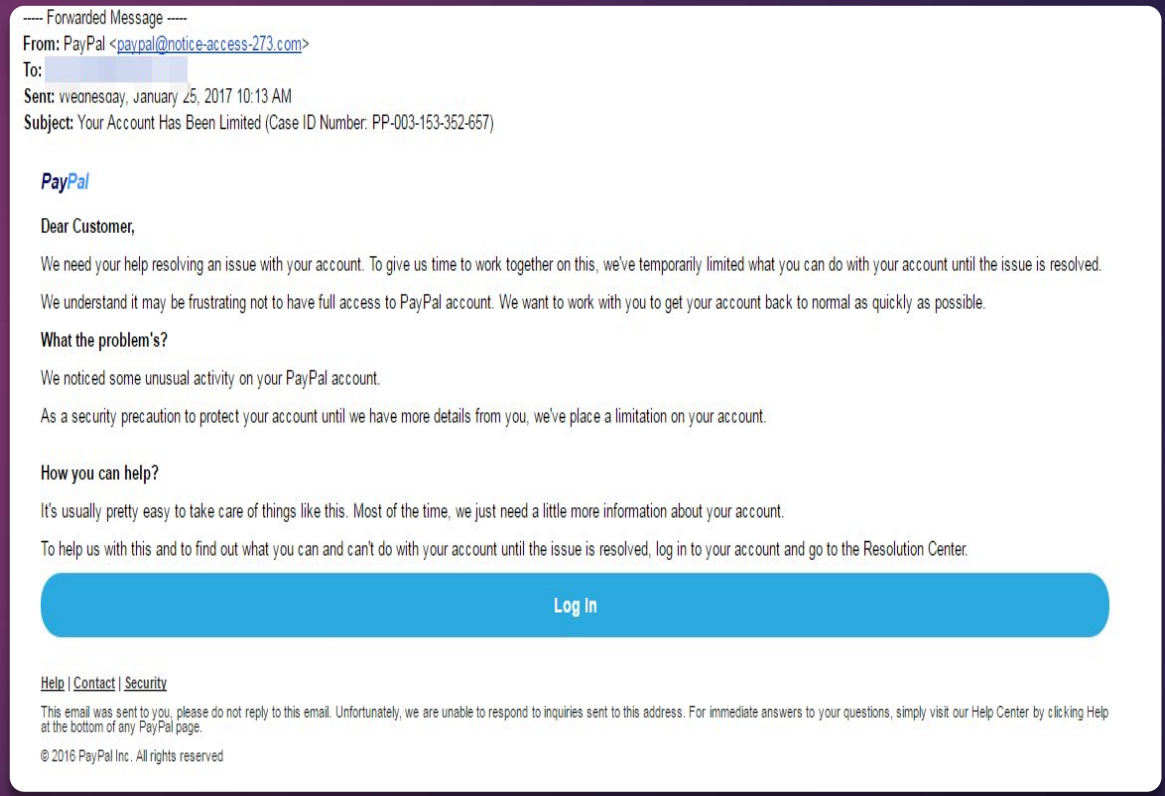
Office 365 - Update

Dear user

This message is being sent to you to inform you that your account is to be closed

If you wish to continue using this account please upgrade to our services.
Ignoring this message will cause your account to be closed

Update your account



---- Forwarded Message ----
From: PayPal <paypal@notice-access-273.com>
To:
Sent: Wednesday, January 25, 2017 10:13 AM
Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Log In

Help | Contact | Security

This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

© 2016 PayPal Inc. All rights reserved

Top Tips to Avoid Phishing

- Check who the email sender is
- Check the email for grammar and spelling mistakes
- Hover over the link with your mouse to see where the link will send you (it will show you the website address the link will open)
- Do not click the link – manually type it in
- Look for Urgent or Threatening Language – phishing messages often create a sense of urgency, like threatening to close accounts or imposing fines unless you respond immediately

Threats Overview

What is "Social Engineering"?

- Manipulation of people into divulging confidential or sensitive information
- Most commonly done over email, but also regularly carried out over the phone
- Can be a slow gain of information
- Can attempt to gain all information needed at once

Social Engineering Examples

- Phone call targets employees at a business
- Caller asks who the boss/CEO is
- Requests his/her email address
- Now the attacker has the username and the name of the person targeted for compromise
- Victims are bombarded with fake threats and warnings that their system is infected with malware, prompting them to install software that has no real benefit (other than to the attacker) or is malware itself

Social Engineering Examples

- **BEC Scam**: An attacker will send an email that appears to come from a senior colleague or a significant business partner. The email typically requests wire transfers, payment of invoices, or access to employee tax records.
- **Pretexting**: In this scenario, an attacker invents a scenario to engage a targeted victim in order to steal their personal information or gain access to their property. For example, an attacker may impersonate a co-worker or a bank official to solicit personal information under the pretext of a mandatory verification process.
  - A person walks into office pretending to be a contractor
  - Due to his/her uniform, people assume it's okay
  - Person walks into a room with sensitive info and steals it

Top Tips to Avoid Social Engineering

- Be careful with the information you disclose
- Verify the credentials of contractors
- If you have any doubts about the identity of callers, hang up and call their official company number back

Users and Poor Password Hygiene

Typically, users practice risky behavior with respect to passwords.

Passwords nowadays can be a gateway into identity theft.

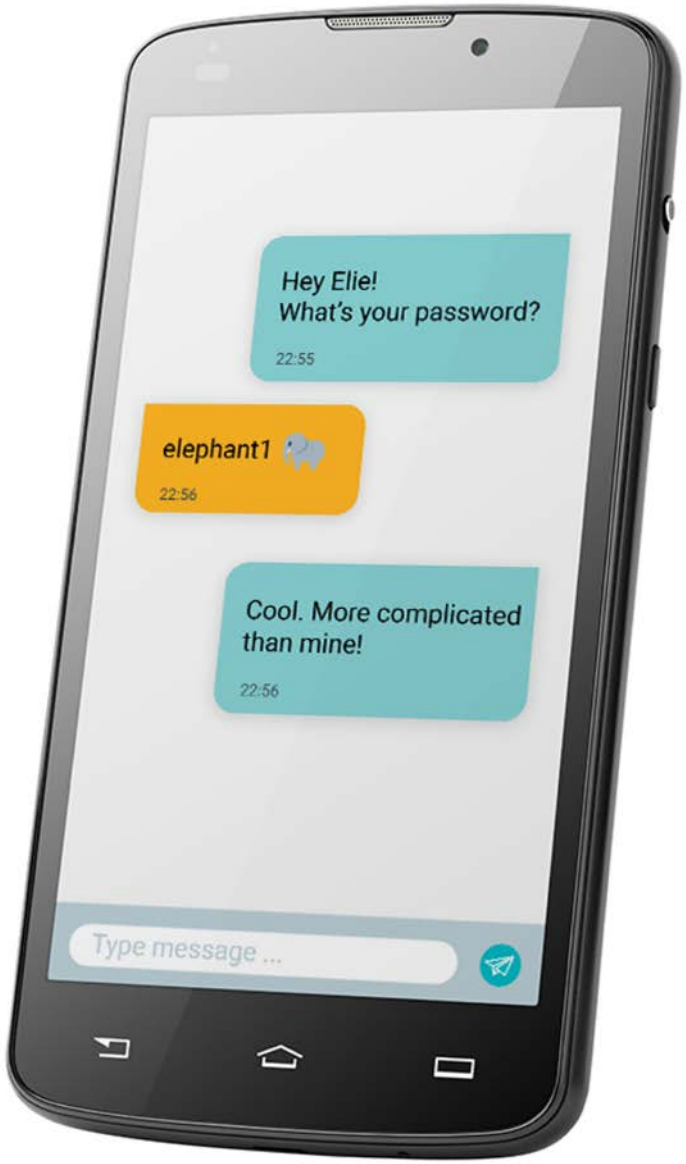
Data Accessibility

- Do you document your password on a sticky note?
- Or do you have it a saved in your agenda or a notebook?
- These are common methods to mitigate getting into a difficult situation if you forget your password
- But they represent a security risk

- Where you document your username and password information is important
- Consider if it's publicly accessible to anyone
- That information should always be kept confidential

Data Accessibility

- Do you freely **share** passwords with friends or family members?
- Do you have shared passwords?
- Do you have a shared record for passwords like a notebook or a dry erase board?

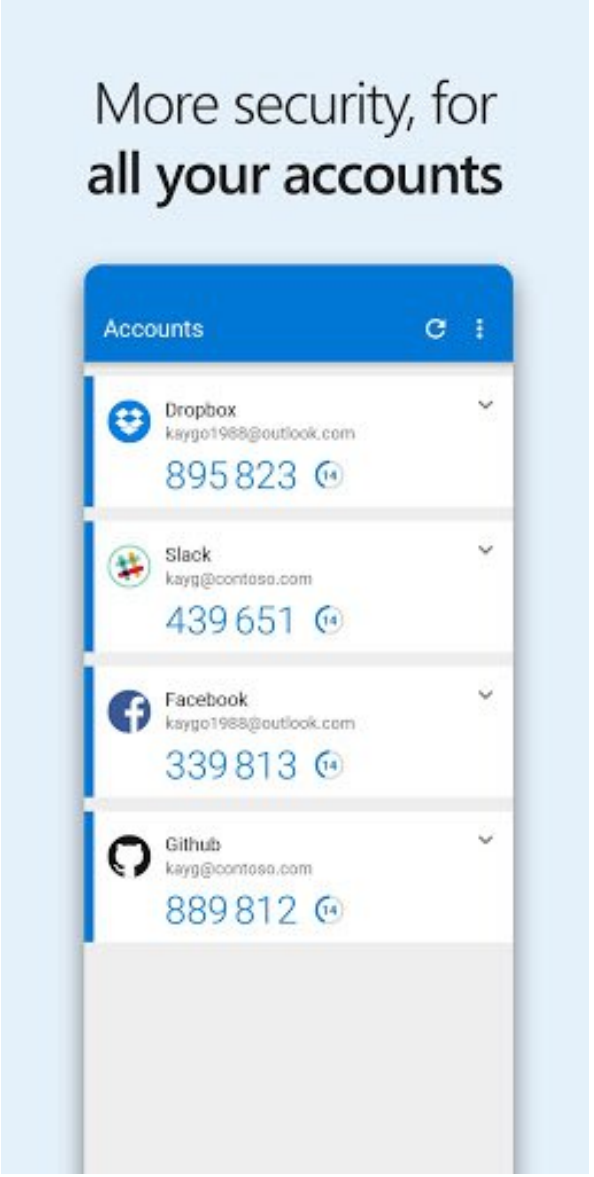


Data breaches lead to password problems because…

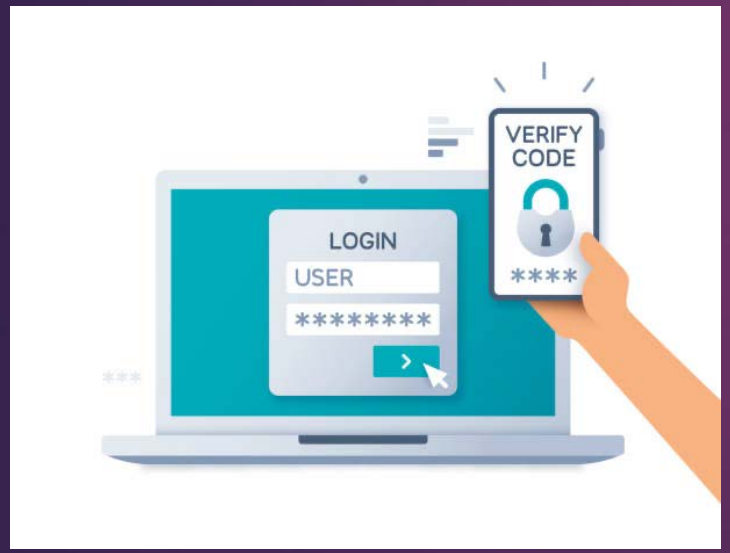
- Passwords can be extracted
- It's very simple to try all alternative options of a password-base
- Example:
  - Password that was stolen was "elephant"
  - Password required by website is 8 characters 1 symbol
  - With 32 symbols on the computer, it would take a human 5 minutes to try out all possible combination
  - Computers can carry out these tasks in fractions of a second
- A website can check if your account was compromised:
  - https://haveibeenpwned.com/
  - Currently checks 280 websites
  - 5.0 billion compromised accounts contained
  - Treat it like a credit-check

Two-factor Authentication (2FA) Explained

- As opposed to the standard password authentication, 2FA OTP (one-time password) uses two elements
- These are "*something that the user knows*" – such as a password or a PIN code, and "*something that the user has*" – typically a mobile phone or hardware token
- Used in combination, they provide greatly enhanced security for data access



2FA solves the problems of:



- Data breach through weak or stolen passwords
- User-created passwords that are not random characters
- Re-use of passwords intended for access to company assets for private accounts
- Passwords containing user-specific data – ex. name, date of birth, etc.
- Simple patterns to derive new passwords, such as: “elephant1,” “elephant2,” etc.

Top Tips for Password Safety

- Use unique passwords across all websites/applications
- Enable and utilize 2FA on all websites that allow it
- Choose unique, non-true security questions

Top Tips for Search Engines

- Stick to clicking on sites on the first page of results
- Be careful when clicking on non-name recognizable sites
- Malware commonly masquerades as free things – don't click on things that say they're "free"

2FA (Two-Factor Authentication) and Email

- Email is the most important account needing protection, because if someone gains access to your email, they can use the password reset function to gain access to other services
- As we mentioned earlier, 2FA is a great way to protect your email from being compromised
- Lullaboo enables 2FA on all email accounts

Top Tips for 2FA and Email

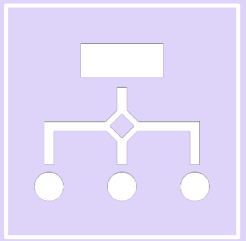
- Password protect or utilize fingerprint reader to protect your 2FA app in case of a lost device
- Do not use SMS if you can help it as a 2FA method – instead use an application or push
- Enable 2FA not just on email, but all critical websites and applications that allow it

Spam Protection

- Everyone gets spam; even with the best protection, some still slips through the cracks
- Some email providers have better spam protection than others
- Never open spam emails, even if you think it is funny to see the content inside
- Never respond to spam emails
- Be careful using your email address to sign up for contests or enter websites

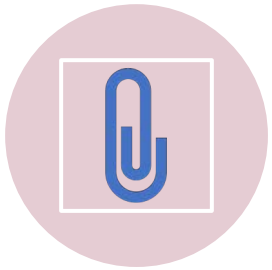
Top Tips for Spam Protection

Never click, open, or respond to spam messages



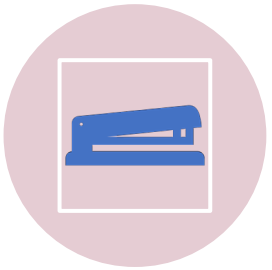
When sending an email to a classified site, use the following format to keep spam bots from retrieving and using your address: john.smith (at) email.com

Email Protection Overview



RULES SHOULD BE IN PLACE AT YOUR COMPANY TO PREVENT RECEIVING CERTAIN TYPES OF ATTACHMENT FILES.

EMPLOYEES SHOULD RECEIVE TRAINING THAT DESCRIBES WHY ATTACHMENTS CAN BE HARMFUL.



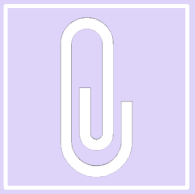
NEVER OPEN ATTACHMENTS FROM UNKNOWN SENDERS.

IF YOU SEE SOMETHING THAT IS QUESTIONABLE, SEND TO YOUR IT DEPARTMENT FOR VERIFICATION.

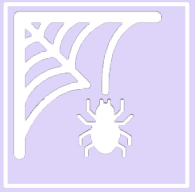
Attachment Policy

- Attachments are one of the most common ways to get viruses or malware
- Even though an attachment might look like a document or Excel file, it might contain a virus or malware
- Rules should be in place at your company to prevent receiving certain types of attachment files
- Employees should receive training that describes why attachments can be harmful
- Never open attachments from unknown senders
- If you see something that is questionable, send it to your IT department for verification

Top Tips for Attachment Policies

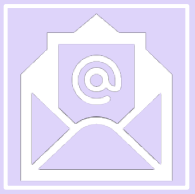


Never open or save attachments from an unknown sender



Even though something looks like a file that you do not think is malicious, it doesn't mean it isn't malicious

Report Suspicious Emails



Follow company protocol for reporting phishing attempts to itsupport@lullaboo.ca

Never respond to or forward suspicious emails