EMAIL – who still uses it?

Email is still one primary way we communicate especially with companies/organizations where we do business.

SPAM: is commonly used to conduct email fraud.

Email spam, also known as junk email, is unsolicited bulk messages sent through email. Hackers collect data about you on the Internet (web sites, newsgroups, and social media) to build mailing lists.

Fraudulent spam - The advance-fee scam is a well-known example -- a user receives an email with an offer that purportedly results in a reward. The fraudster presents a story where they ask for money from you. When payment is made the fraudster will invent further fees, or stop responding.

Phishing – An email used to trick the recipient by making it seem legitimate. It may contain an attachment or link in the message. Opening or clicking may install malware (harmful program or file) on the your device or direct you to a malicious website set up to trick you into divulging personal and financial information, such as passwords, account IDs or credit card details.

Malware types: virus, worm, Trojan horse, spyware, ransomware, adware, malvertising. All of these have unique traits and characteristics with how they work but, their end goal is to collect user data and observe your activity without your knowledge.

Remember traditional email has few privacy protections; your email can be read by anyone who gains access to it… like a postcard.

Protecting Yourself: take time to really read the email as there are usually clues in the email that point to some form of SPAM.

- The email creates a sense of urgency, demanding “immediate action” before something bad happens, like closing your account. The attacker wants to rush you into making a mistake without thinking.
- You receive an email with an attachment that you were not expecting or the email entices you to open the attachment. Examples include an email saying it has an attachment with details of unannounced layoffs, employee salary information or a letter from the IRS saying you are being prosecuted.
- Instead of using your name, the email uses a generic salutation like “Dear Customer.” Most companies or friends contacting you know your name.

AUTHENTICATION: Passwords are the weakest link when it comes to email or applications.

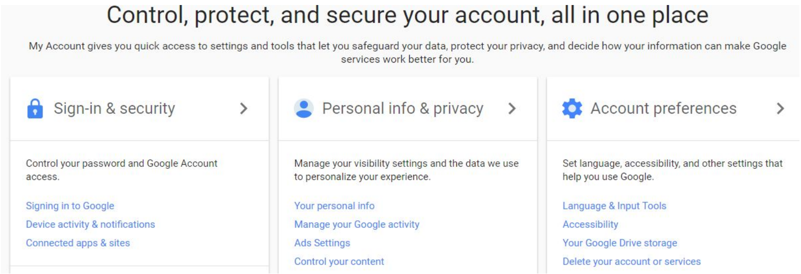
What can I do to improve my Email security and privacy?”

1. Use 2 factor Authentication… everywhere. Most of us use a Google product or two. Two-step, or two-factor authentication protects your accounts by requiring you to provide an additional piece of information after you give your password to get into your account. In the most common implementation, after correctly entering your password, an online service will send you a text message with a unique string of numbers that you’ll need to punch in to get access to your account.

   ****Use this on every account you have that offers it. Ex. Twitter, Slack, PayPal, Microsoft accounts, Facebook, Evernote, Dropbox, Apple, etc.**

   Google: Log into your account click your avatar in top right corner.

   - go to **MY ACCOUNT**
   - under sign-in & security **Signing in to Google**



Control, protect, and secure your account, all in one place

My Account gives you quick access to settings and tools that let you safeguard your data, protect your privacy, and decide how your information can make Google services work better for you.

Sign-in & security

Control your password and Google Account access.

Signing in to Google
Device activity & notifications
Connected apps & sites

Personal info & privacy

Manage your visibility settings and the data we use to personalize your experience.

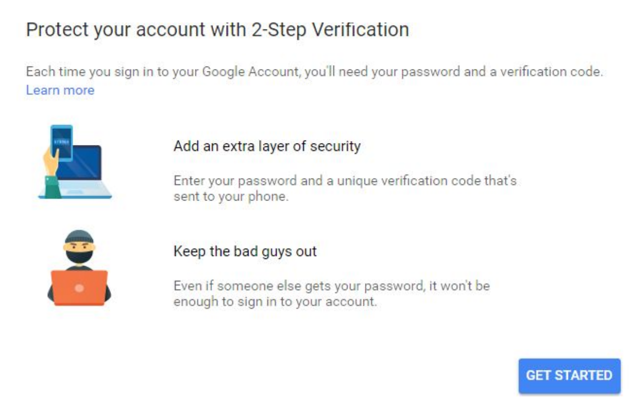
Your personal info
Manage your Google activity
Ads Settings
Control your content

Account preferences

Set language, accessibility, and other settings that help you use Google.

Language & Input Tools
Accessibility
Your Google Drive storage
Delete your account or services

   - Enable 2-Step Verification, then **GET STARTED,** then enter your password, then select your method of receiving the code… text or call.



Protect your account with 2-Step Verification

Each time you sign in to your Google Account, you'll need your password and a verification code.
Learn more

Add an extra layer of security

Enter your password and a unique verification code that's sent to your phone.

Keep the bad guys out

Even if someone else gets your password, it won't be enough to sign in to your account.

- click **NEXT**, if you chose text you'll get a **CODE**, enter it, then click next.
- if it worked the next screen will confirm, then click **TURN ON,** done.

The last screen gives you other options like setting up **backup phone** in case your phone is ever unavailable. If you lose your phone this is a good suggestion just let the person know you are using them as your backup.

2. Notifications: go back to **MY ACCOUNT** these let know when there are changes to your account.
   - click Device activity & notifications.
   - then **MANAGE SETTINGS,** in the Security alert settings box.
   - Check the boxes to receive alerts by phone or email.
   - Choose **Done**.

3. Connected apps & sites: this is also under Device activity & notifications. Check every often to see what apps you may have signed in to with your Google account.

4. Passwords: SIZE MATTERS …Everyone knows you reuse the same password for everything, because it's easy to remember. A password manager can help to randomize strong passwords and store them securely. Use this software to randomize and quickly fill out your unique passwords.

   ****Use the password manager for every password and just on your email.
   Ex. Facebook, Dropbox, Slack, etc.**

   My favorite is LastPass – Free https://lastpass.com/misc_download2.php
   It supports Windows, Mac, iOS and Android devices. https://lastpass.com/features/
   - 256 bit encrypt & two-factor
   - Local only encrypt - User data is encrypted and decrypted at the device level
   - Online password generator - https://lastpass.com/generatepassword.php

   Another free:

DashLane Password Manager - supports Windows, Mac, iOS and Android devices.

- 256 bit encrypt
- Free - http://keepass.info/download.html - open source

1Password – is popular and supports the same devices but, it is not FREE.

https://1password.com/

Other good tools to use:

Have I accidently loaded Ransomware on my device?
https://ransomfree.cybereason.com/

Has my email account been hacked? https://hacked-emails.com/

What should I do if my email is hacked? Even with the steps taken above hackers are getting smarter and finding new ways to get our information or money.https://www.webroot.com/us/en/home/resources/tips/getting-started/beginners-what-do-i-do-when-my-email-has-been-hacked-and-spam-is-sent-to-my-contacts

Check out this link to do 2-factor authentication on some other popular applications.
http://gizmodo.com/its-time-to-enable-two-step-authentication-on-everythin-1646242605