Gmail Security Checklist

To make sure your Gmail account is secure; take a minute to complete a Gmail security checklist to make sure your mail security measures are up to date.

Your Computer

Check for viruses and malware

While no virus scanner can catch 100% of infections, it is still important to run a scan on your computer with trusted anti-virus software (or install a program that runs in the background and scans continuously). If the scan detects any suspicious programs or applications, remove them immediately. Some good free programs are Microsoft Security Essentials (Windows Defender in Win8), AdvancedSystem Care 7 and Malwarebytes. There are many others.

Microsoft Security Essentials is a free and reliable real time anti-virus program that can be downloaded at http://windows.microsoft.com/en-US/windows/security-essentials-download

Advanced SystemCare 7 is a free **on demand** malware program that can be downloaded at http://www.iobit.com/advancedsystemcareper.html

Malwarebytes is also a free **on demand** malware program that can be downloaded at http://www.malwarebytes.org/

There are also paid versions of Advanced SystemCare 7 and Malwarebytes.

YOU SHOULD ONLY RUN **ONE** REAL TIME ANTI-VIRUS PROGRAM ON YOUR COMPUTER. If you have more than one antivirus program running at the same time--or more than one firewall--you're asking for trouble. Two such programs, trying to do the same thing at the same time, will slow down your system. Worse, they can cause conflicts.

Make sure your operating system is up to date

Operating systems release patches to repair security vulnerabilities. Whether you use Windows or Mac OS, we recommend protecting your computer by enabling your automatic update setting, and updating when you get a notification.

Make sure to perform regular software updates

Some software updates aren't included in your operating system updates, but they are just as important. Software such as Adobe Flash and Adobe Reader release regular updates that may include repairs for security vulnerabilities.

An excellent free program is Secunia PSI found at http://secunia.com/ The Secunia Personal Software Inspector (PSI) is a free computer security solution that identifies vulnerabilities in non-Microsoft (third-party) programs which can leave your PC open to attacks. Simply put, it scans software on your system and identifies programs in need of security updates to safeguard your PC against cybercriminals. It then supplies your computer with the necessary software security updates to keep it safe. The Secunia PSI even automates the updates for your insecure programs, making it a lot easier for you to maintain a secure PC.

Your Browser

Make sure your browser is up to date

To check for browser updates in Internet Explorer, select the **Tools** tab and click **Windows Update**. In Firefox, just click the **Help** tab and select **About Firefox**. Google Chrome automatically updates when a new version is released; however you can also select the google menu bar and then select **About Chrome.**

Check your browser for plug-ins, extensions, and third-party programs/tools that require access to your Google Account credentials

Plug-ins and extensions are downloadable computer programs that work with your browser to perform specific tasks. For example, you may have downloaded a plug-in or extension that checks your Gmail inbox for new messages. Google can't guarantee the security of these third party services. If those services are compromised, so is your Gmail password.

Your Gmail Account:

Change your Password and Update Account Recovery Options, 2 Step Verification and Authorized Applications and Sites

Password:

If your account has been recently compromised, you should update your **password** now. In general we suggest you change it periodically, following these guidelines:

Pick a unique password that you haven't previously used on other sites or on Gmail. Just changing one character or number still counts as reusing your password.

Don't use a dictionary word or a common word that's easily guessable. Use a combination of numbers, characters, and case-sensitive letters.

Account Recovery Options:

We all may forget our passwords at some point, so we strongly encourage that you update your **account recovery options.**

Google can use your recovery email address to communicate with you if you lose access to your account.

2 Step Verification:

2-step verification adds an extra layer of security to your account by requiring you to sign in with something you know (your password) and something you have (a code sent to your phone).

Authorized Websites:

Make sure that the list of authorized websites are accurate and ones that you have chosen. If your Google Account has been compromised recently, it's possible that the bad guys could have authorized their own websites to access your account data. This may allow them to access your Google Account after you have changed your password.

To change or verify any of the above:

Click the **gear icon** ⚙ in the upper right, and then select **Settings**.
Click **Accounts and Import**.
Go to **Change Account Settings**
Click on Other Google Account Settings
Click on Security
Edit specific field

Use a secure connection to sign in.

In your Gmail settings, select 'Always use HTTPS.' This setting protects your information from being stolen when you're signing in to Gmail on a public wireless network, like at a cafe or hotel.

Click the **gear icon** ⚙ in the upper right, and then select **Settings**.
Click on the **General** tab.
Go down to **Browser connection.**
Place selection on **Always use https.**

Check for any strange activity on your account

Go to your Inbox and go to the bottom of the page. Click the Details link next to the **'Last Account Activity'** entry at the bottom of your account to see the time, date, IP address and the associated location of recent access to your account. Also make sure you have selected "**Show an alert for unusual activity**", so you will be notified if Google finds unusual activity on your account.

At the top of this box there is a place to "**Sign out all other sessions**". If you select this box it will sign you out of your Gmail account on all devices. This is particularly helpful if you lose a mobile device.

Final Reminders

Watch out for messages that ask for your username and/or password. Gmail will never ask for this information.

Keep secrets! Never tell anyone your password.

Only select 'Stay signed in' if you're signing in from a personal computer.

To sign out of your account, click on your picture and select "**Sign out**". If you have synced your data on a computer *other than your own*, make sure you select the menu bar, select "**Settings**" and select "**Disconnect your Google Account**".