



A Simpler
Guide^{TO}

ONLINE SECURITY

for
Everyone!

How to protect yourself and stay safe from fraud, scams and hackers with easy cyber security tips for your Gmail, Docs and other Google services

Ceri Clark

A Simpler Guide to Online Security for Everyone

How to protect yourself and stay safe from fraud, scams and hackers with easy cyber security tips for your Gmail, Docs and other Google services

Ceri Clark

Copyright © 2015 Ceri Clark.

This ebook is licensed for your personal use only. This e-book may not be re-sold or given away to other people. If you would like to share this book with another person, please purchase an additional copy for each person. If you're reading this book and did not purchase it, or it was not purchased for your use only, then please return to the online retailer and purchase your own copy. Thank you for respecting the hard work of this author.

[Click here for the full copyright and publication information.](#)

About the Author

Ceri Clark is a full-time author and mother. She was a Librarian with over eleven years of experience in corporate, public and private libraries culminating in a Library Manager position at the ill-fated English Audit Commission. Following the closure of the library (and the demise of the organization) she began to utilize her skills for searching, writing and advising with her 'A Simpler Guide to' series.

Other books from Ceri Clark

A Simpler Guide to Calibre:

How to organize, edit and convert your eBooks using free software for readers, writers, students and researchers for any eReader

A Simpler Guide to Finding Free eBooks:

A step-by-step guide to discovering and downloading free e-books for the Kindle, Kindle Fire, Android, iPad and other e-readers

A Simpler Guide to Gmail:

An unofficial user guide to setting up and using your free Google email account

A Simpler Guide to Google+:

An unofficial user guide to setting up and using the Google Plus social network

Email Management using Gmail:

Getting things done by decluttering and organizing your inbox with email organization tips for business and home

Coming Soon

A Simpler Guide to Google Drive for Everyone
A Simpler Guide to Google Docs for Everyone
A Simpler Guide to Google Sheets for Everyone
A Simpler Guide to Google Slides for Everyone
A Simpler Guide to Google Forms for Everyone
A Simpler Guide to Google Drawing for Everyone

Children of the Elementi:

Middle Grade/Young adult fantasy.

When an ancient Empire is defeated, its heirs are sent to safety but a hundred years on and they may not as safe as their parents had hoped.

Contents

Chapter 1 Introduction

[Who is this book for?](#)

[*The Student*](#)

[*The Jobseeker*](#)

[*A Small Business*](#)

[*A Charity*](#)

[How should I use this book?](#)

[What services does Google offer?](#)

[*Gmail*](#)

[*Drive*](#)

[*Docs*](#)

[*Sheets*](#)

[*Slides*](#)

[*Forms*](#)

[*Drawing*](#)

[Why do I need to protect my account?](#)

[*How do hackers benefit financially?*](#)

[Chapter Summary](#)

Chapter 2 Passwords

[Choosing your password](#)

[Changing your password](#)

[Chapter Summary](#)

Chapter 3 Two-factor Authentication

[How to setup 2-step verification on Google](#)

[Backup access](#)

[Security Keys \(FIDO\)](#)

[*How do I get a security key*](#)

[*Setting up Google to use your key*](#)

[How do I use a Security Key](#)

[Using Google Services on your mobile device\(s\)](#)

[Accessing 2-step authentication after setup](#)

[Using an Android app to gain verification codes](#)

[Chapter Summary](#)

Chapter 4 Protecting your account away from home

[Use your own devices where possible](#)

[Use sites that connect with https](#)

[Don't trust free Wi-Fi](#)

[VPN Services](#)

[In-private browsing](#)

[Always log out](#)

[Consider not taking your device](#)

[Chapter Summary](#)

Chapter 5 Other ways to protect your account

[Adding recovery information](#)

[Recovery email](#)

[Recovery Phone](#)

[Codes](#)

[Let Google know where you live](#)

[Delete your account](#)

[Chapter Summary](#)

Chapter 6 Phishing and scams

[Recognizing spam, scams and phishing emails](#)

[It's too good to be true](#)

[Your friend is on vacation and asks you for money](#)

[A stranger sob story](#)

[An email sent to yourself](#)

[Bad grammar and spelling](#)

[Bank emails](#)

[The unsubscribe link](#)

[Information you should never share](#)

[Your mother's maiden name](#)

[Social Security number](#)

[Birth date](#)

[Your pet's name](#)

[Chapter Summary](#)

[Chapter 7 What to do if your Google account is hacked](#)

[Check your back up access information](#)

[Change your password](#)

[Setting up 2-step verification](#)

[Check your sent mail](#)

[Chapter Summary](#)

[Glossary](#)

[Index](#)

[More from Lycan Books & Myrddin Publishing:](#)

Chapter 1 Introduction

What to expect in this Chapter:

- > What is this book about?
 - > Who is this book for?
 - > How should I use this book?
 - > What services do Google offer?
 - > Why do I need to protect my account?
-

We are spending more and more time on the internet, putting our data out there in online services. Some of the most trusted services are those provided by Google. While most of what they offer is free, much of what they provide can become invaluable to save time and money in our everyday lives.

When Gmail is used (as with any email provider), it can become a hub for using other websites and services outside as well as in Google. For example if I forget my password for a shopping website, I can get my password sent to me or change it by getting the website to send an email to my Gmail account. Without precautions, this can become a security risk. If an unauthorized user were to gain access to my Gmail account, they could have free rein to get into any website where I have used my Gmail email address - just by asking websites to recover my password. The password gets sent to my email account, they open the email and change the password. The hacker would then delete the recovery email so I would be none the wiser that anyone else has access to my Gmail or that another website is compromised. Depending on how that shopping website was set-up, it could even have my credit card details in it too.

If I protect my Gmail account (and therefore all Google services), it blocks the unauthorized user from using that avenue to get hold of my data, or even using my Gmail account to try and trick my contacts into giving away their information.

Protecting your email account from identity thieves, scammers and hackers should be a priority when dealing with online safety. This applies to all email accounts from all providers and is the first step to securing your personal and financial information across the web.

Who is this book for?

This book is for anyone who has a Google account. This could be anyone who needs email, free storage or productivity tools such as a word processor, spreadsheet or presentation software. Whether you are a student, employee, job seeker, a small business or a charity, are using it for home or work, this book can help you protect your Google account and therefore protect yourself. Here are just some of the reasons why you may have or want a Google account:

The Student

Don't worry about losing that essay half-written again! Google Drive backs-up your essays and papers automatically. No need to pay for expensive subscriptions for office software. You can write your essays with Google Docs, make your slides for presentations with Google Slides and work out your budget with Sheets, all while keeping in contact with your friends and family with Gmail and Hangouts.

The Jobseeker

Use Google Drive to store your résumés and keep track of your job applications. Make and store presentations for interviews and apply using Gmail. All for free!

A Small Business

If you are working to a tight budget then Gmail, Google Drive and its connected suite of office applications can tide you over until you need more. Google offers more space for a fee but with 15GB for free you may not need it for a while.

A Charity

If you are a Charity you will have access to Google's premium model for free. This means your storage will be doubled to 30GB.

How should I use this book?

This guide contains step-by-step instructions on how to protect your Google Services which include Gmail, Google+, Drive, Docs, Sheets, or Slides, among others.

The first chapter discusses how to choose a password and then includes instructions on how to change it. Next, the importance of using 2-step verification (also known as two-factor authentication) is discussed as well as instructions for setting up the 2-step verification is provided. There is really no better way to protect your accounts than to use this facility. The rest of this book concentrates on strategies to protect your account while away and other options that Google suggests.

As well as working out your passwords, hackers will try to trick you into giving them your information for other websites using emails. This is social engineering. The chapter on scams and phishing discusses the most popular of these tricks.

If you have been hacked, chapter 7 talks about what you can do to minimize the damage and how to secure your account again.

As with all books in the Simpler Guide series, there is a glossary and an index at the back so you can quickly find what you need.

For the purposes of this guide, I have made a few assumptions. The first is that you have a computer or a tablet, or at least have access to one. I have also assumed that you are familiar with using a mouse and know what the internet is. If you need detailed notes on how to use Gmail itself, I recommend my A Simpler Guide to Gmail book.

You can access the security options discussed on this guide on a phone or tablet but when setting up your security for the first time, I strongly recommend you do this on a computer for the ease of access. The reason for this is that the interface may change for different makes of phone and mobile devices, while Google has full control of how their website looks on a browser on a computer. This means the interface will remain consistent unless of course they change it for their own reasons.

This leads me to a small disclaimer at this point. Google constantly changes the services it offers. It is constantly evolving and while this book is as accurate

as could be made possible at the time of publication, the security options covered by this book can and will change. Features will be added and others taken away, however, the principles will remain the same.

If you have bought this book as a Kindle book, I recommend downloading the Kindle for PC/Mac programs from Amazon (free) to view the book from your computer. You will be able to click on links and the images will be of better quality.

What services does Google offer?

Google's strength is that it has many integrated services it provides for free. This section talks about what Google offers and what you are protecting when you implement the security measures outlined in this book. If you are considering going through the Google or Microsoft route (why not use both services) then this section may sway you.

Gmail is Google's answer to email. It is one of the best and the closest competitor is Microsoft's Outlook and Office suite. Google Drive is at its heart storage. It is a means of saving your files in the cloud. This means your files are kept on Google's computers, which are always online. The advantage of this is that you can access your files from anywhere there is an internet connection.

Docs, Sheets and Slides are productivity tools, which can be used with just a browser. This means you do not need to download anything to use these tools. They are similar to Word, Excel and PowerPoint. Google+ is a social network similar to Facebook and Twitter.

One Google account will access all these services and more. Here is a brief description of Google's most popular services:

Gmail

Gmail is Google's email service. Use their fantastic tools for organizing your emails. Find out more in [A Simpler Guide to Gmail](#).

Drive

A computer folder kept on Google computers where you can store your files. The advantage of using Google Drive over a folder on your computer is that your files will be saved automatically and available from anywhere there is an internet connection. Coming soon: *A Simpler Guide to Google Drive*.

Docs

Docs is a word processing application similar to Microsoft Word, Works or Apple's Pages. Again this is available anywhere there is an internet connection, including mobile device(s). Coming soon: *A Simpler Guide to Google Docs*.

Sheets

Sheets is a spreadsheet application, a way to manipulate and display numbers. It can automate calculations and create charts. Sheets is the free alternative to Microsoft's Excel program. Again this is available anywhere there is an internet connection, including mobile device(s). Coming soon: *A Simpler Guide to Google Sheets*.

Slides

Slides is Google's answer to presentation software. Similar to Microsoft's PowerPoint, Slides can be created which tell a 'story' or illustrate points when making a presentation. Again this is available anywhere there is an internet connection, including mobile device(s). Coming soon: *A Simpler Guide to Google Slides*.

Forms

Forms gives you the ability to collect information by creating forms and surveys, which can be filled in from the internet. They can be created with no programming skills or experience needed. Coming soon: *A Simpler Guide to Google Forms*.

Drawing

Drawing is an online tool for creating charts and other graphics. The nearest Microsoft product to this is Microsoft Visio. Coming soon: *A Simpler Guide to Google Drawing*.

Why do I need to protect my account?

Securing your Google account is very important. The sum of all your emails, documents, posts, contacts and other data can help someone to take advantage of you or use your details for their own use. Identity theft is a growing problem on the internet and in real life and you need to protect yourself as much as possible.

There are a couple of reasons why someone may want to access your account. The main one is financial but another is because they can. There are people who think of breaking into other people's accounts as fun but mean no harm.

How do hackers benefit financially?

While there are people who will break into other's websites, bank accounts and email accounts for fun, there is usually a financial motive behind the behavior. Listed below are a few of these.

Identity Fraud to get loans

This is linked to getting your social security number. If someone can get enough accurate information about you. With for example, your birth date, your full name, your address, your social security number (in the USA) etc., the hacker can build a profile and use it to trick financial institutions to change your address and lend them loans or gain access to services they wouldn't normally have access to, such as health insurance and loans.

Getting your Credit Cards

Using your Gmail account, they could access other accounts where they could possibly get hold of these numbers. This could be a shopping site, which doesn't store your card details as securely as they should.

Getting your Social Security Number

In the US, hackers may try to get hold of your social security number. This would give them access to loans *etc.* In other countries, a social security number is not used as the gold standard for identification as it is in the USA so this may not be applicable to readers outside of the States.

Harvesting your friends' and colleagues' email addresses

Email addresses are big business. There are databases being sold illegally on the internet for spammers, scammers and hackers. Your friends' details are valuable.

Sending email to pretend they are you

This is a popular scam. A fraudster will log into an account and send an email to a friend. They say you are abroad and that you have been stranded/mugged or lost all your money. They will then ask your friend to send you money through a money transfer service or direct to their bank. They will then delete the email to your friend so that you can't warn your friend in time.

Your friend at this point is worried about you and sends money without checking that you are actually on vacation. Depending on your friends' generosity, this could be quite lucrative.

Using Google Voice to make phone calls

If you have a Google Voice account, hackers could use this service for long distance phone calls or even for more scams.

Corporate spying

It may sound far-fetched but a competitive company could hire a nefarious hacker to peruse your documents to steal your ideas, business processes or contacts. By protecting your accounts, you can help to keep this information to yourself.

Chapter Summary

Financial fraud, identity theft and just malicious hacking are rife on the internet. There are things you can do to protect yourself. This guide is a step-by-step guide to being proactive and improving the security on your Google account to make life difficult for the people trying to do the same to you.

Google accounts are for everyone, students, jobseekers, small business and even charities. Keeping these accounts secure helps to protect your and other people's information, and to keep your money and your peace of mind out of the hands of hackers. Using the security tools that Google provides, can make your Gmail account, and other Google products, one of the most secure and productive services you can have on the internet.

Chapter 2 Passwords

What to expect in this chapter:

> Strategies for choosing your password > How to change your password

This chapter is all about the password. While passwords are important, they are only one tool in protecting your account. Alone, they can be hacked.

Together with two-factor authentication, they are a powerful preventative and will scupper many a would-be opportunist hacker.

Choosing your password

Your password needs to be strong. There are a few schools of thought when it comes to thinking up passwords, so here I am going to cover five ways. Whatever you choose, there should be a *minimum* of 8 characters in your password. If possible, these should be a mixture of lower and upper case letters, numbers and special characters such as a \$, *, &, @ *etc.*

Option 1:

The simplest one to remember is choosing three random words, which mean something to you but would be impossible to guess for an outsider. For example, if your favorite food is cake, your favorite vacation was in Hawaii and you just love baseball, then as much as my spell check hates it, *cakeHawaiiibaseball* could be considered a reasonable password.

Option 2:

Another way to choose a password is by using a combination of letters, numbers and special characters. Using everyday words can make it easy to remember. For example, *Elephantsrock* is bad, but *El3ph@nt5r0ck* is strong. To get *El3ph@nt5r0ck*, I replaced an e with a three, the a with @ symbol, s with five and o with zero. All the replacement numbers look like their letter counterparts to make it easy to remember.

Option 3:

The third way is to choose a phrase, which you will remember and take the first letters of each word. For example: *The scariest movie I have seen is Omen!* Once you have settled on a phrase just add a special character and number. I saw the film when I was about 9 so that's the number I will choose here. This password would be: *TsmihsiO!9*

Option 4:

Another way to choose a password is similar to the above method but involves an aid. Those familiar with the 2011 movie *Unknown* starring Liam Neeson may recognize this. If you have a favorite book then choose a passage and from that passage choose a word. For example, if the word is in the 22nd line on page 150, two words along and the word is mammoth, the word would be 150222mammoth, or any combination of these elements that is easy for you to remember.

Option 5:

Another method to create a highly secure password is to create a spreadsheet on your computer and record all your passwords. The secret here is that you only type half of the password in your file. What you record needs to be random with a combination of characters. The reason that this method is secure is that half of the password is only stored in your head. It does not matter where you put the memorised half of the password into the complete password (at the beginning or end) as long as it is not written down. An example could be: *Memorised half (only in your head):* wind *Recorded half (in spreadsheet):* Hydf54j@#f *Full password while logging in:* windHydf54j@#f As you can see this would be difficult to guess. You should not store it in a password vault service unless you put it behind something protected by 2-step authentication.

Tip If you are like me and are liable to forget passwords, a good way to cheat is to use a service such as LastPass. Sign up at lastpass.com and use their service to either generate passwords for you or to remember passwords you have made. You will need one password to use LastPass but the service will remember all your other login information and can automatically log you in to websites.

This way you can have different passwords for all the websites you visit and only have to remember the one! The service will also warn you when websites have been known to be compromised and ask you to change your password for them.

I would like to say a word of warning though. If you use this service make sure that you set up the password recovery options. You will need to install the LastPass plugin and have setup the recovery information. The service is very secure and if you have not done this and you have lost or forgotten your

password, then there is no way of getting back your password database. You can generate a one-time password for emergencies.

To be very secure with LastPass, set up two-factor authentication. This means that you will need both a password and your phone (or other physical device) to be able to login. A hacker will not usually have access to your phone and if they do steal it from you, you will still be protected by the password. If your phone was stolen, you would then automatically change your password and use the recovery information to regain access to Lastpass.

Changing your password

To change your password on your Google account at any time: *Step 1:* Go to your profile picture (on the top right of the screen).



Figure 1 Go to My Account

Step 2: Then select *My Account* as above.

Step 3: Click on *Sign-in and Security* in the first box you see.

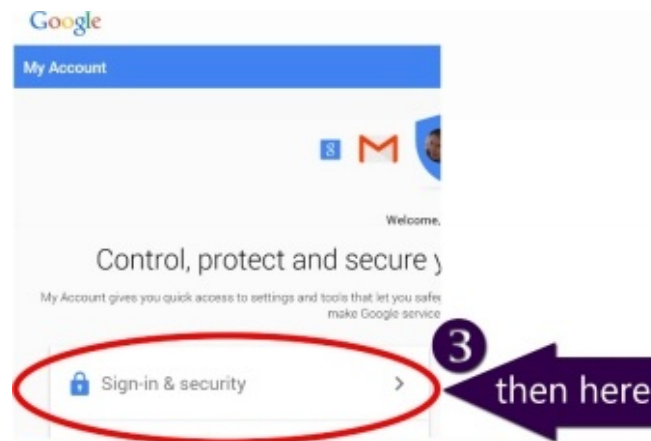


Figure 2 Go to My Account

Step 4: Scroll down the page until you see the password section on the right side of the page. Choose *Password*.

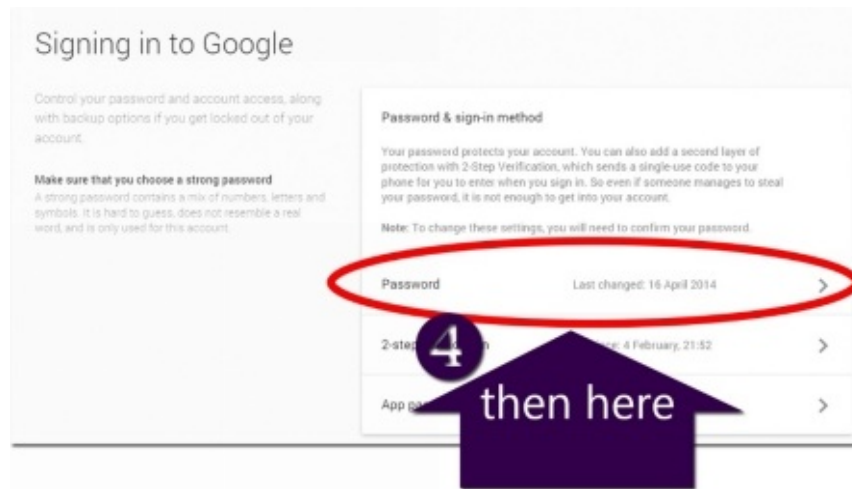


Figure 3 Go to My Account

Step 5: Login to your Google account with your current password when you are prompted.

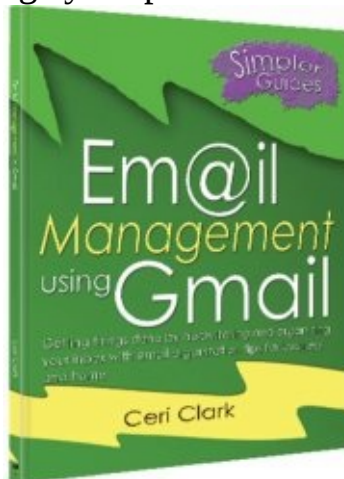
Step 6: Type in your password in the first box and again in the second and then click on *Choose Password*.

Your password is now changed. Once this is done, any devices using your Google account (phone) will ask for the new password.

Chapter Summary

There are various different ways to choose a secure password. At the very least they should be 8 characters minimum and a combination of letters, numbers and special characters. A special character is one which isn't part of our normal alphabet, like the @, ! or % symbols. Varying which characters are upper and lower case also beefs up the strength of your characters.

The second half of this chapter gives you step-by-step instructions on how to change your password on your Google Account.



Discover the power of Gmail for organizing your email



AVAILABLE AT
amazon

Chapter 3 Two-factor Authentication

What to expect in this Chapter:

- > Setting up 2-factor authentication (otherwise known as 2-step verification) > What are security keys, how do get them and how to use them > Getting verification codes from your phone
- > How to get to 2-step-verification after setup

Changing your password regularly is a good way of securing access to your account, but remembering hundreds of passwords, constantly changing, can be a headache. Google's two-step verification can be an elegant solution to this for access to their website. However, for really strong security, using both a good password and two-factor authentication is a great choice.

2-step verification/authentication is an extra step to make sure that access to your information, files and folders is restricted to you. Instead of relying just on a password (which might be acquired through nefarious means by hackers), a second device is used which you always have on you such as a phone, tablet computer or key ring. Any would-be infiltrator, bent on your destruction would need to have your password AND your phone to gain access to your account.

How to setup 2-step verification on Google

Step 1: Go to your profile picture and click on it.

Step 2: Click on *My Account* as seen below.



Figure 4 Go to your My Account

Step 3: Look for the section labelled *Sign-in and security* and click on it as seen below.

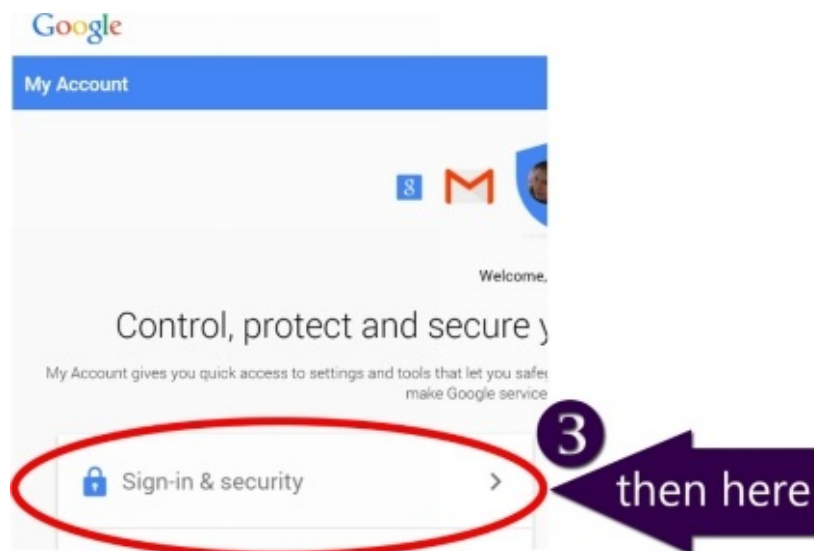


Figure 5 Go to Sign-in and Security

Step 4: Click on *2-Step Verification* as seen in the next graphic.

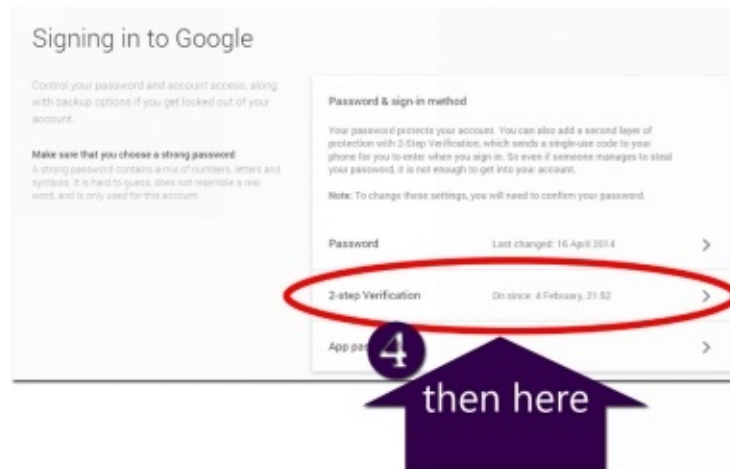


Figure 6 2-step verification setup location The following page will load.

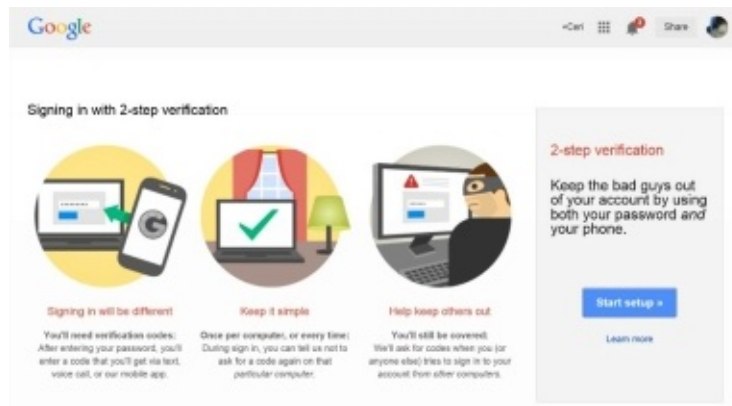


Figure 7 2-step verification welcome screen Click on Start Setup in the box on the right of the screen and you will be directed to login again. Once you do, you will be taken to the page to setup the verification.

Type in your cell/mobile number in the space provided (making sure the correct flag is chosen to represent your country code *i.e.* stars and stripes for the US and the Union Jack for the UK) as illustrated in the next figure. Next, choose how you want the code to be sent to you. I chose SMS text verification. Click *Send code* and the code will be texted to you.

Figure 8 Enter your cell/phone number

Take the code from your phone and enter it in the space provided in the form and click *Verify*.

Figure 9 Enter the verification code

Check your phone and put in the code that was texted to you in the box provided, as seen above. Google will then ask you if you trust the computer that you are on. If you share a computer, say in a student house or an internet café then you should *uncheck* the box that says *Trust this computer*.

Lastly, for the setup, confirm if you trust the computer and that you understand that you will need to use special codes if you use other computers.

The following page will load:

2-Step Verification





Verification codes	App-specific passwords	Registered computers	Security Keys
PRIMARY WAY YOU RECEIVE CODES			
	Primary number <div> <div>Your cell no.</div> <div>Edit</div> </div>		
	Codes sent via: <div>Text message</div>		
	Added on: <div>Aug 19, 2015</div>		
<div>  <div> Get codes via our mobile app instead Our app for Android, iPhone, or BlackBerry even works when your device has no data or phone connectivity. <div>Switch to app</div> </div> </div>			
BACKUP OPTIONS FOR WHEN YOUR PRIMARY IS UNAVAILABLE			
	Backup numbers ⓘ <div> <div>No backup phones</div> <div>We strongly recommend that you add at least one backup phone.</div> <div>Add a phone number</div> </div>		
	Backup codes ⓘ <div> <div>No backup codes printed or downloaded</div> <div>We suggest that you print or download backup codes, especially if you travel or have problems receiving codes on your phone.</div> <div>Print or download</div> </div>		

Figure 10 2-step verification settings

Your account is now protected using the 2-step verification system. As it is set-up, you will need to type in a code that Google will text you every time you want to login to your Google account. To save you doing this every time you want to check your email, you can register the computer (which really registers the browser you are using) when it prompts you.

If you use Firefox when you registered Chrome, you will need to register that browser as well. You can check what computers (browsers) that you have asked Google to remember by clicking on the *Registered Computers* tab at the top of the page as can be seen in the above graphic.

It is possible to use an app on your phone rather than get text messages. This is useful if you live somewhere where you cannot get a phone signal. Please see the section called [Using an Android app to gain verification codes](#) for more information on how to do this.

Once you have logged in to your Google accounts on your phone, for

checking your email in the Gmail app for example, it is treated as a trusted device and will not ask you for any 2-step verification codes.

Backup access

Of course, the main point of 2-step verification is to make it impossible to access your Google accounts but you don't want to be locked out of your own account either. This is why adding a backup phone and having backup codes will be a lifesaver when you really want access but you can't receive text messages, or you don't have the authenticator app on a smartphone.

This is important because if you lose your phone and need a 2-step verification code, the second phone can be used to regain access to your account.

To add a backup phone number, click on *Add a phone number*. The rest is self-explanatory.

To get Backup codes, click on *Print or download* and a list of back up codes will be generated as in the next figure.

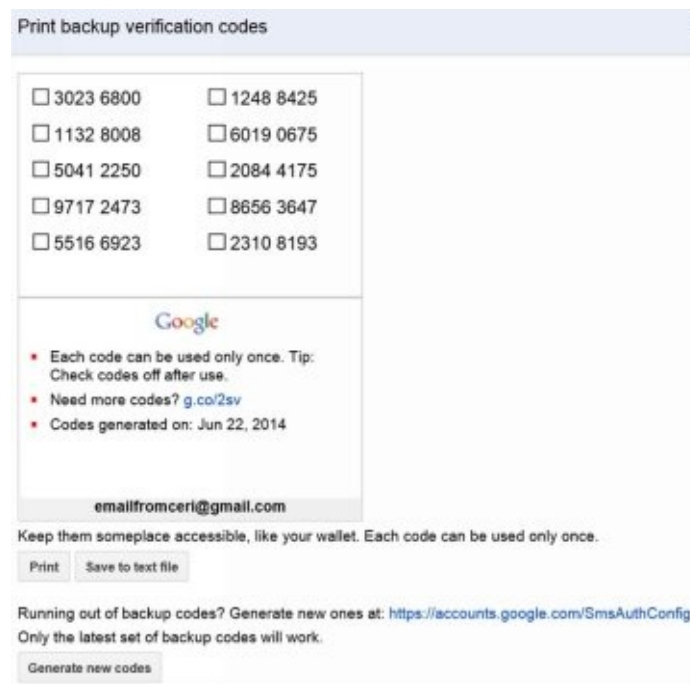


Figure 11 2-step verification settings

You can print these out or save them to a text file.

Don't lose these and remember each code can only be used once. To generate more application specific codes simply click on *Generate new codes* on

the bottom of the page.

Security Keys (FIDO)

Security keys are a relatively new way of protecting your account. They are a physical device as big (or smaller) than a small USB flash drive. It can fit on your key chain and can be used instead of your mobile phone or tablet as your second factor for entering your Google account.

How do I get a security key

Amazon sells these. Look for a FIDO compatible key. FIDO is the security standard that Google uses for device based 2-factor authentication. You can buy keys from as little as \$6, and up to \$50 with NFC built in. NFC is a wireless standard you can use with your cell phone to transmit a code to your phone. NFC allows you to use your key on your mobile phone, thus if you just want to use your key to access Google on your computer you can just buy a \$6 key.

Setting up Google to use your key

Ensure that you are using your Google Chrome browser and: *Step 1: Go to your profile picture > My Account > Sign-in and security > 2-Step Verification > Security Keys (fourth tab across)* *Step 2: Click on Add Security Key* *Step 3: Click on Register* *Step 4: Insert your key into a USB port in your computer and press the button on the key* *Step 5: Click Done*

How do I use a Security Key

Open Chrome to login to your account. When prompted after you have put in your password, put in your security key and press the button on it.

A new code is generated each time the button is pressed. The sequence, which the key generates is unique to your key.

Using Google Services on your mobile device(s)

If you use apps on mobile devices for any Google service, you will need to have application specific passwords for apps which aren't compatible with 2-step verification, to be able to access Google from them.

If you only access Google from your computer you do not have to worry about application specific passwords.

You will need to generate some passwords that will only need to be inputted once for each application on a device. Click on *App specific passwords* tab on the top of the page and then *Manage application-specific passwords*.



Figure 12 Manage your passwords for your mobile device(s).

You will of course be asked to login again.

In the past, I have used my Gmail account on my smartphone and tablet using a third party email app. To use the app I had to generate a password. I typed *MailDroid Phone* (MailDroid or K9 are good 3rd party email applications) in the box provided on the webpage that loaded.

Authorized Access to your Google Account

Application-specific passwords

Some applications that work outside a browser aren't yet compatible with 2-step verification and cannot ask for verification codes, for example:

- Apps on smartphones such as Android, BlackBerry, iPhone, etc.
- Mail clients such as Microsoft Outlook
- Chat clients such as Google Talk, AIM, etc.

To use these applications, you first need to generate an application-specific password. Next, enter that in the password field of your application instead of your regular password. You can create a new application-specific password for each application that needs one. [Learn more](#)

[Watch the video on application-specific passwords](#)

Step 1 of 2: Generate new application-specific password

Enter a name to help you remember what application this is for:

Name:

ex: "Bob's Android", "Gmail on my iPhone", "GoogleTalk", "Outlook - home computer", "Thunderbird"

Figure 13 Generating passwords for apps

Once you have typed the application name click on *Generate password*. On the next screen your one time only password will appear as illustrated in the next figure:

Authorized Access to your Google Account

Application-specific passwords

Step 2 of 2: Enter the generated application-specific password

You may now enter your new application-specific password into your application.
Note that this password grants complete access to your Google Account. For security reasons, it will not be displayed again:

pbdw wrpi akeo txws
No need to memorize this password.
You should need to enter it only once. Spaces don't matter.

Your application-specific passwords	Creation date	Last used date	
MailDroid Phone	Jun 22, 2014	Unavailable	[Revoke]

Figure 14 2-step authentication passwords generated screen

Notice that the application that you specified appears at the bottom of the screen? This is the beginning of a list of passwords you will have to generate for every application on all your mobile devices that you want to connect to Google. Click on *Done* to generate more passwords.

Google allows you to *Revoke* the password at any time by logging into your account. By doing this, if you lose your phone/tablet or other device then you can delete the passwords stopping anyone from accessing your account from that device.

If you have more than one device where you use the same application (for example, K9 on a tablet *and* a phone) I would recommend that you put the

device name in the application name you chose. For example, you could use K9Phone or K9Tablet depending on your preference.

Now that you have your password, type it in to the password field of the application that you want to use on your device.

For MailDroid, I clicked on the email address, chose *Edit* and typed in the confirmation code without spaces into the password field. I was able to refresh the email as normal.

A word of warning, if you use MailDroid or another application that downloads your email, even if you use 2-step verification, someone could still access information already downloaded on to your phone.

Even if you have put a generated password in the application, information already on there can still be accessed after you have revoked the password. However, they won't be able to download new emails, therefore 2-step authentication should not be used as a replacement for password protecting your device and enabling encryption.

Accessing 2-step authentication after setup

To get back into your 2-step authentication go to:

Your profile picture > My Account > Sign-in & Security > 2-step Verification

Using an Android app to gain verification codes

Every 30 days you will be asked to re-login, this also happens if you use a computer you haven't used before. You can get codes by SMS or using an Android app (Authenticator or Authy). This section explains how to use *Google Authenticator*.

First install "Google Authenticator" from Google Play/Play Store (this used to be also called the Android Market) on your Android device, or App Store on your iPhone.

Step 1: In Google Play, search for *Google Authenticator* *Step 2:* Click on *Install*.

Step 3: Go back to your 2-step verification administration panel in your computer browser by going to *Your profile picture > My Account > Sign-in & Security > 2-step Verification* *Step 4:* As you will be using Google authenticator, click on *Switch to app* as seen in the next figure.



Figure 15 Switch to Google Authenticator

Step 5: Select the phone type from the options that pops up. In my case, it was Android.

If you are using an iPhone or Blackberry, follow the on-screen instructions for those devices. Click on *Continue*.

A page will load with a barcode.

Set up Google Authenticator

Install the Google Authenticator app for Android.

1. On your phone, go to the Google Play Store.
2. Search for **Google Authenticator**.
(Download from the Google Play Store)
3. Download and install the application.

Now open and configure Google Authenticator.

1. In Google Authenticator, touch Menu and select "Set up account."
2. Select "Scan a barcode."
3. Use your phone's camera to scan this barcode.



[Can't scan the barcode?](#)

Once you have scanned the barcode, enter the 6-digit verification code generated by the Authenticator app.

Code: [Verify and Save](#) [Cancel](#)

Figure 16 (Step 5) Mobile app authentication page

Step 6: Go back to your mobile device and choose *Begin setup*.

Step 7: Next, press on *Scan a barcode*.

Google's or another barcode scanning application will load. If you don't have a barcode reader already on your device, Google will suggest one and direct you to download it.

Step 8: Use the camera on your device to view the barcode on the computer screen. Google Authenticator will then give you a unique code to type into the box labelled *code* at the bottom of the barcode page on your computer.

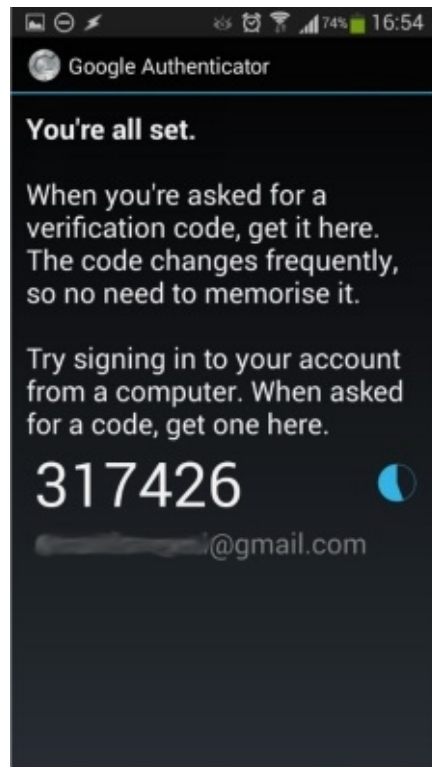


Figure 17 Google Authenticator code from a mobile device After you click Verify on your computer, you will receive a message to say your Android device is configured.

If you find that it doesn't work after a few attempts check the time and time-zone is correct on your mobile device.

Chapter Summary

Two-step verification is the gold standard for protecting your account. It means that should someone guess your password, then they need your mobile device to get access and vice versa. If they have stolen your mobile phone they will need your strong password.

This chapter also shows how to use app specific codes to get to your Google account from mobile devices and how to use your phone to get the second verification you need to get into your account.

Chapter 4 Protecting your account away from home

What to expect in this Chapter:

> Using your own devices > Protecting your data whilst and after you use your device > About VPN services and how to find them

It is difficult to disconnect completely from the internet when we are away from home. It is just too tempting to have a quick check to see if any new emails have arrived. Considering a few things when you want to check your email or other accounts while away from home can keep your accounts secure.

Use your own devices where possible

If you are staying in a hotel or going to an internet café, try to use your own phone, laptop or mobile device.

By using your equipment, you know (if you have taken the right security precautions such as anti-virus software) that no malicious software has been installed before you get there to view your screen or record what you type. Using your own equipment easily eliminates a set of threats to your security.

Use sites that connect with https

When you connect to a site on the internet, you can either view the website on a protected (https) or unprotected address (http). The 's' in https stands for secure. It means that the connection is encrypted so that only you and the site you are visiting will see what you are doing. A 'listener' may see that you have visited your bank but they will not be able to see your passwords or anything that you are doing while you are there.

If you can, and if the site supports it, you should always log on to a website using https.

Don't trust free Wi-Fi

Free wireless is a godsend when your mobile has run out of data. When you are on vacation you may want to Skype or hangout on Google, if you do, 3G is not as good an option as using your hotel's Wi-Fi. My advice is not to trust the Wi-Fi blindly but take steps to protect yourself.

The reasons that free Wi-Fi can be dangerous are:

- it may not be configured correctly
- it may be a fake or a honeypot Wi-Fi at a train station for example (a honeypot is a trap, where they pretend to be a trusted wireless source solely to gather and steal your details)
- there may be adverts served by your hotel which helps to pay for it but which could contain viruses without the hotel's knowledge
- or it could just be someone has found a way to get around security and are using the wifi to listen to what people are doing on it.

There are services, which allow you to 'tunnel' from your device to a website. While you are in the tunnel no one can see what you are doing. These are called VPN services. There are free as well as non-free versions available. If you are worried about security these can be very useful.

Use 3G on your phones when possible or apps that encrypt what you are sending and receiving information online.

VPN Services

VPN stands for virtual private network. Services spring up all the time but also disappear as quickly. There are a number of VPN services available on the internet. These are secure ways of browsing the internet. You are protected in a tunnel that encrypts your data and location.

Some are paid and other are free. A paid service that is good is *Pure VPN* (<https://www.purevpn.com/>). The price is just short of \$50 with discounts for a year.

To find a good VPN service, search for *VPN* on Google and look for reputable reviews. PC Mag for example had an article for The Best VPN Services for 2015 at <http://www.pcmag.com/article2/0,2817,2403388,00.asp>.

In-private browsing

If you are in an internet café or a shared computer then you should use in-private browsing in your browser. This means that when you close the browser, all the login information is gone. Using this option means, someone cannot go back in to the history and have a look at what you were doing. This does not protect you from listeners/watchers but protects you after you have finished browsing.

Always log out

Again if you are using a shared computer or in an internet café, log out of any services you are using when you are finished.

This also applies when you are away and using your own devices. If your device gets stolen then if you have all the security hints enabled in this book (2-step verification) then they shouldn't be able to get into your accounts.

If for any reason you cannot follow all these tips then your 2 step-verification will protect you up to a point. Somebody may see what you have been doing while you were online but what they can do with that information is limited. They will not be able to login to your account later and wreak havoc.

Consider not taking your device

This may seem contrary to earlier advice in this chapter but you may want to work on your laptop and your company requires that your computer is encrypted. If you are going to Russia or Brunei for example, you will be required to have an unencrypted device to enter the country. If you do this then your data is exposed which may be against your company's policy or interests. The only way around this scenario is to not take your laptop in the first place.

Chapter Summary

Google services can be accessed from anywhere you can connect to the internet. This includes while on vacation as well as popping out for some shopping. There are a few things you can do to increase your security while accessing your account while you are out.

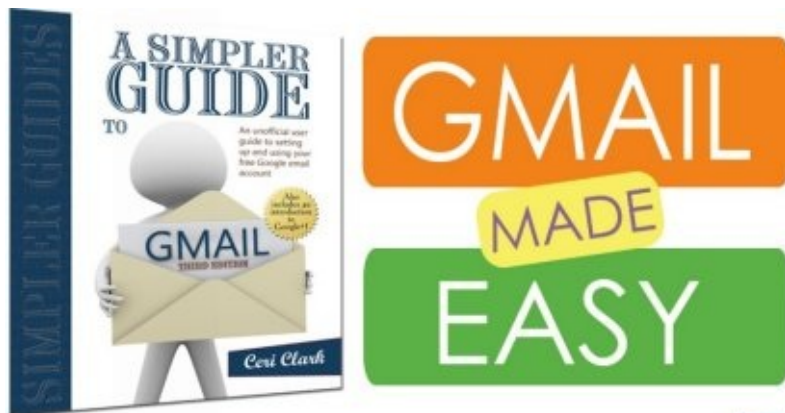
The first and easiest way to secure your account is to always use your own devices. You can't always be sure that everyone else is as conscious as you are about security and their computers could be riddled with viruses and they might not even know it.

Visiting websites using a secure connection is another way to keep safe. If the website shows https in the address bar you are far safer than if it has http at the beginning of the web address.

The Wi-Fi you use at home will be secured but you cannot guarantee that a free Wi-Fi by any other source will have the same security. There are people who will take advantage of this but you can use VPN services or your own data connection such as 3G to thwart listening attempts.

If you are using shared computers and internet cafés then using in-private browsing and logging out of a service will also protect you.

There are occasions when leaving your laptop at home is your only option.



A
step-by-step
guide to
getting the
most out of
Gmail



AVAILABLE AT
amazon

Chapter 5 Other ways to protect your account

What to expect in this Chapter:

> Adding recovery information > Letting Google know where you live >
Deleting your account

It is very important to add recovery information and let Google know where you live. The first is essential so that if you are locked out of your account for any reason there is still an 'in' to it and you can reset settings to enable you to login in easily again.

If you let Google know where you live, they will let you know if someone has logged in to your account from a different location. You can then take steps to change passwords and revoke codes.

Adding recovery information

If you haven't added ways to get your account back, if you forget your password when you set up your account, then you can do this by going to: *Your profile picture* > *My Account* > *Sign-in & Security* Look down the page until you see the box entitled, *Account recovery options*.

Click on the arrow next to each option to add the information.

Recovery email

If you have more than one email address, you can put one of your other addresses in here. If you don't you can set up a new one from Outlook.com or use a trusted family member or friend's email address. It is a good idea to use a different person's email address or from a different email system so it is completely separate. You must really trust a friend to use their address as this is a security threat in itself if they take advantage of you.

Recovery Phone

Put your mobile phone in this section. You could use your landline but using a mobile number will be more convenient if you are out.

Only one phone can be inputted in the first screen but if you click into *2-step verification* above the current box, you can add more numbers in the box labelled *BACKUP OPTIONS FOR WHEN YOUR PRIMARY IS UNAVAILABLE* (their caps not mine!). Click on the button *Add a phone number*.

Codes

Make sure you have a copy of your generated codes. Keep these in a safe place. You can always revoke the current codes and generate new ones if you need to though.

To get to your backup codes go to *Your profile picture* > *My Account* > *Sign-in & Security* > *2-step Verification* and go down to the last option on the page.

Let Google know where you live

Keeping your personal information up to date is important for your overall Google security. If you let Google know where you currently live then they can inform you if your account has been accessed from elsewhere. If you are living in Florida but your account was accessed from Mexico, you know something is up!

Google likes to use your IP address to locate you but they sometimes get this wrong. To put your address in manually, go to Google Calendar:

Menu (button with 9 squares in 3 x 3 square format) > *Calendar* > *Gear wheel* (top right of browser) > *Settings*

Scroll down to *Location* and type in where you live.

There is also an option in Google+ to update your address but you need to make sure that it is only visible to you as you don't want everyone to know where you live.

If you follow most, if not all, of the suggestions in this book you will have secured your Google account from all but the most dedicated hacker. All that is left to say is keep an eye on your account for suspicious activity every now and again and you have done everything you can.

Delete your account

Protecting your account can also mean maintaining access to it. If you cannot get in to your account then you cannot make sure that no one else is. If you no longer need an account, delete it completely from Google's services. Ghost accounts are a security threat.

Please make sure that the account you are about to delete is not used to login to any sites or as security verification for a service. You will not be able to use those again if it is. In addition, all information will be deleted and you will not be able to get it back. You can however download your information before clicking on the fateful button.

To delete your account, please follow these steps:

Step 1: Click on your profile picture on the top right of your screen Step 2: Click on My Account Step 3: Click on Delete your account or services under My preferences Step 4: Delete Google Account and data Step 5: Login and read the page.

Step 6: Click on DELETE ACCOUNT

Chapter Summary

Even with the best of intentions, it is possible to lose a password or something can go wrong. If this happens to you, you will have needed to make sure that you put recovery information on your account *before* you lost access. This is a priority. The important things you need to put in are another email address, a phone number and to have generated codes for the 2-step verification.

Google should know where you live and they will send notifications if your account is logged in from elsewhere. If for some reason this has gone wrong you can set your location using Google Calendar as explained in the above chapter.

Would you like a free book? I'm building my email list to let readers know when I release new books. As a thank you for letting me update you on my progress, I am giving away a full copy of my e-book, *A Simpler Guide to Finding FREE eBooks*. The book may change at any time so check out my website at <http://cericlark.com> to see what the latest freebie is!



A SIMPLER GUIDE
TO
Finding
FREE eBooks

**YOUR
FREE
eBOOK**

FIND FREE EBOOKS

For a limited time, you
can get a **FREE** copy of
A Simpler Guide to
Finding **FREE** eBooks

<http://cericlark.com/subscribe/>

Chapter 6 Phishing and scams

What to expect in this Chapter:

> How to recognize spam, scams and phishing emails > Information on popular scams > What information you should never share

Using passwords, 2-step verification and the other methods outlined in this book can protect you from opportunist hackers. There is another way to extort money from you, which involves tricking you into giving personal information. The only way to avoid these sophisticated scams and phishing emails is to be aware of them and be wary of opening emails and clicking on links from email senders you are not familiar with.

Recognizing spam, scams and phishing emails

Spam, scams and phishing emails can be a security risk. They change all the time. The spammers/phishers get more sophisticated as time goes on but there are some things that make these messages stand out. This section is just some of the things you can look out for in these types of emails. Be aware that Google will NEVER contact you to verify your details. If you strongly believe that an email is from Google, do not click on any links but go direct to your Google account and change details on their website.

It's too good to be true

If you receive an email from a Nigerian prince/princess letting you know that they are in trouble but they will give you several million but only if you give them your bank details - this can be a good indication.

Another famous email scam is a foreign lottery/competition letting you know that you have won millions. This would be fantastic but if you have never bought a ticket, how likely is this to be true?

There are variations on these themes but they usually involve offering a large amount of money in unlikely circumstances.

Your friend is on vacation and asks you for money

This is a scam where your friend's email account has been hacked and an email then sent to you stating that s/he is in trouble on vacation and could you send them a couple of thousand to help him/her out? If you get any emails like this, check that they have actually gone on holiday first!

If this has happened, tell your friend that his/her account might have been hacked. The hacker may have deleted all sent emails so it may not be obvious to them that there was a problem. They will need to change their password straight away and maybe enable 2-step verification.

A stranger sob story

A stranger is dying/ill/in trouble. Please send money quickly. I would ignore these emails. How did they get your address?

An email sent to yourself

In the past, I have sent emails to myself to remind me to do things. If there is one person I trust it is me! If I am very distracted it is not beyond the bounds of possibility that I could click on one of these emails by mistake. There is a scam where people have faked the email address so it looks like you have sent an email to yourself. Think before clicking on any links!

Bad grammar and spelling

A telltale sign of a malicious email is bad grammar and poor spelling. If you get an email with these features, handle with care.

Bank emails

Your banks will never ask you for personal information by email. They will also never give you a link to click on to log in. If you receive emails that ask for this, use a direct link you already have. These are usually on letters and statements from your bank.

Some of these emails will say your account has been hacked, some money has gone missing or something along these lines. They will encourage you to click on a link in their email which will take you to a special website which will look like your bank's website but will be owned by the scammers. These emails are known as phishing emails. They will ask you to put in your username and password, which they will then record. You will be redirected to your actual bank and you will probably not know what has happened until your real bank contacts you by phone or letter.

The way to avoid this is never to click on any link in an email that appears to be from your bank but to go and have a look at your bank's website directly.

The unsubscribe link

Most of the time you will receive emails that you have signed up for in the past. You may not want them anymore but they are not spam as you originally asked for them. To stop receiving these, click on the unsubscribe link which is usually at the bottom or top of emails that have them.

Occasionally you will receive offers, promotions and other emails where you do not remember signing up. If this happens to you, do not use the unsubscribe link. This is because these are spam messages used to try and get your details. Sometimes it is just to see if your email address is genuine. A good give-away for this is if your name is in the CC of the email (for example John Smith) but you can also see John A Smith, John B Smith, Jonnie smith *etc.* in there. They are trying every combination they can think of to get a hit. Other times it is to get other information such as a username or password. If you have different passwords for every website this is not a problem but a lot of people keep the same password for many sites. Once they get hold of *that* password, they have access to all the websites which use the password and this could be banks or stores.

Information you should never share

Whether you are asked via email, facebook, by phone or someone with a clipboard questions you on the street, there are some pieces of information that should never be shared. These can be used against you if the questioner were so inclined. They can be used to open bank accounts or break into accounts you already own.

Never share this information but if you do, make something up. If I am asked my mother's maiden name, I never use her real name. I use a name I heard on some random TV program that I saw when I first came up with the idea. If anyone breaks into any one of my online accounts and uses that piece of information, they won't be able to use that answer on my bank's website or in a branch. It will be wrong. The same with birth dates *etc.*

Your mother's maiden name

This is a bad question to begin with. Someone could request your birth certificate or look on a genealogy website for this information.

Social Security number

In the United States, this information can be used to take out loans in your name.
If at all possible always keep this to yourself.

Birth date

If you want to put your date of birth on a website, try changing the year or the day before or after your actual birthday. You can still get the nice birthday wishes but you won't have to worry about your online security in the same way.

Your pet's name

This is a difficult one. You may want to have pictures of your favorite companion on Facebook or Twitter. The answer to this is to have a false name on your bank's website or service rather than the other way around. Just do not forget it!

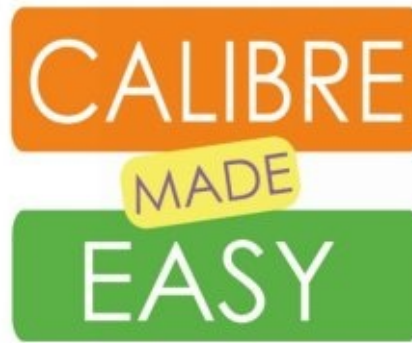
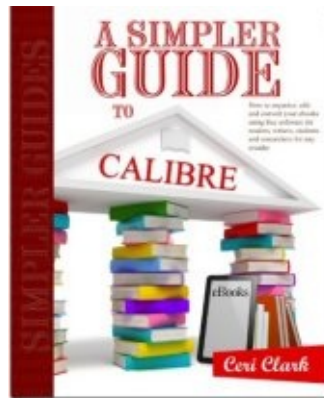
If you feel that you might forget details that you have made up, put the information on a secure medium. Somewhere where you use 2-factor authentication is good as a last resort. The safest way is always to remember it.

Chapter Summary

Social engineering is the means to get you to give out security information that can be used to defraud you. This can be to pretend to be you to obtain loans.

A popular way to get this type of information is to send you emails to get you to fill in online forms, or trick you into sending them money. If it is too good to be true - on the internet it nearly always is.

Use fake information on social network sites, websites and even banks to keep your identity safe. The goal is to make sure that only you know the answer to a security question. It doesn't have to be 'right', just the answer you originally set up.



Make your
own library
catalog and
convert
ebooks with
Calibre



AVAILABLE AT
amazon

Chapter 7 What to do if your Google account is hacked

What to expect in this Chapter:

> Checking your back up information > Changing your password > Set up 2-step verification > Check your sent mail

If you have not had time to implement the recommendations in this book and you have already been hacked or you believe you might be, there are still things you can do.

Follow these steps to lock out any hackers and to secure your account for the future.

Check your back up access information

Your back up information is what you can use to get at your account if your password fails or you lose your phone. If you believe that your account has been compromised then you need to check that only your email address and phone number are in there. A trick that hackers use is to put in their information in the back up section so that if you change your password, they will just change it back again later. You do not want the hacker to know you have changed your password for him or her to change it again and this time lock you out.

To check that the information recorded in Google is yours, go to:

Your profile picture > My Account > Sign-in and recovery > Account recovery options

Change your password

Once you have checked that your hacker won't be notified of you changing your password you will need to actually change your password.

To change your password on your Google account at any time:

Step 1: Go to your profile picture (on the top right of the screen).

Step 2: Then select *My Account*.

Step 3: Click on *Sign-in and Security* in the first box you see.

Step 4: Scroll down the page until you see the password section on the right side of the page. Choose *Password*.

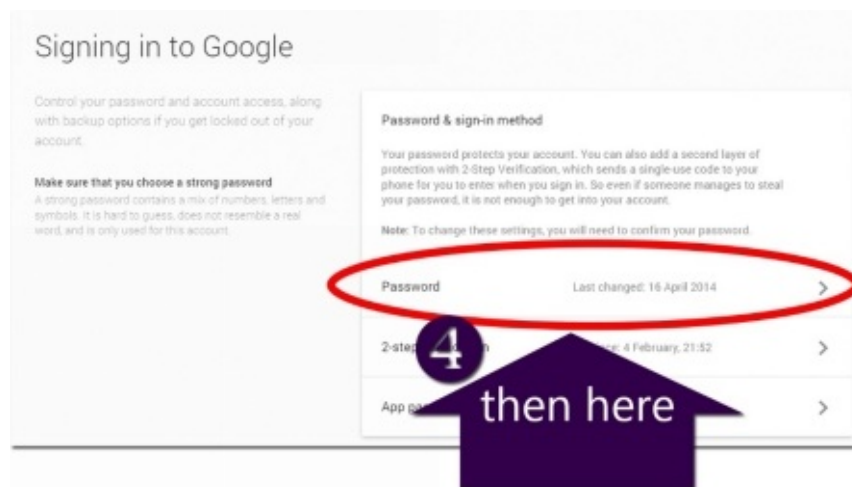


Figure 18 Go to My Account

Step 5: Login to your Google account with your current password when you are prompted.

Step 6: Type in your password in the first box and again in the second and then click on *Choose Password*.

Your password is now changed.

Setting up 2-step verification

The next thing to do is to set up your 2-step verification. This can be done using the password you have changed and one other device. This can be your cell/mobile phone or a security key. This will stop most hackers. Please see [Chapter 3 Two-factor Authentication](#) for detailed instructions for how to do this.

Check your sent mail

Finally yet importantly, have a look in your Sent mail to see if the hacker has sent any emails to your contacts. If you see one, send another email explaining you have been hacked and you are now back in control.

Chapter Summary

Most of what you can do for security is preventative but what can you do if you have already been hacked? First, you need to login to your account and check that the back up security information on the account is yours. Next, you need to change your password and enable 2-step verification. Finally, you should check your sent mail folder to see if the hacker has sent any emails from your account. If they have, you should inform the recipient that you have been hacked

A personal request

If you found this book useful, please help to spread the word. Reviews are the life-blood of an author's career. It is how people can tell if a book is any good. I am a reader as well as an author and if I see a well-written review, I am more likely to give a book a try. I really appreciate the time that a reviewer takes to share their views as much as I enjoy writing these books.

Glossary

2-step verification A security feature where two items are needed to log in to a website. This is usually a password and some other form of identification such as a code from a mobile device.

Address bar The box at the top of your browser where website addresses show, for example <http://gmail.com>

Android device These are smartphones and tablets which run on Google's operating system, Android.

App Short for application, these are small programs which run on mobile devices such as smartphones and tablets.

Browser This is a computer program that allows you to view webpages.

Captcha Also known as word verification, this box, usually containing letters or numbers is used to prove that people submitting to a website are not in fact automated scripts otherwise known as robots.

Docs is a word processing application similar to Microsoft Word, Works or Apple's Pages.

Drawing is an online tool for creating charts and other graphics.

Drive A computer folder hosted by Google where you can store your files. The advantage of using Google Drive over a folder on your computer is that your files will be saved automatically and available from anywhere there is an internet connection.

Export This is a feature where you can download some data or a document that can be saved on your computer which can then be used on a different account or application.

File Explorer An application on your computer which allows you to find files, folders, and software on your PC or Mac.

Forms gives you the ability to collect information by creating forms with no programming skills or experience needed.

Gear Wheel The symbol located on the top right of Google pages that will take you to the settings for that service.

Gmail The free email service provided by Google.

Hackers There are good or bad hackers but for the purposes of this book, I refer to those nefarious people who have devoted their lives to harming you or

others by breaking in to computers.

Homepage The start page of a website, also known as the main page.

Icon A picture or symbol which when pressed takes you to another webpage or function (such as a Google Hangout).

Identity Fraud This is where personal information is stolen and used by a fraudster to take over someone's identity for illegal use.

Images Photos, pictures and graphics.

Import This is a feature where you can upload some data or a document to a web service like Gmail or Google+.

LastPass This is a service from lastpass.com where you can store all your passwords in the cloud which is protected by one password and 2-factor authentication for extra security. Use this service to generate a different password for every website you sign up to but you will only have to remember the one.

Password A string of letters and numbers which can be a phrase or random characters which allows you access to a website or service.

PC A computer that runs the Windows operating system.

Profile In the context of this book this is your information held by Google.

Recovery Information Your recovery information may include backup phone numbers, email addresses and codes that will enable you to get in to your account if you lose your phone or forget your password.

Sheets is a spreadsheet application, a way to manipulate and display numbers. It can automate calculations and create charts. Sheets is the free alternative to Microsoft's Excel program.

Slides is Google's answer to presentation software. Similar to Microsoft's PowerPoint, Slides can be created which tell a 'story' or illustrate points when making a presentation.

Two-factor authentication *See 2-step verification*

URL is short for Uniform Resource Locator. It is a quick way of saying web address.

Username A unique piece of information used as a means to identify you to Google.

VPN is short for Virtual Private Network. It is software that encrypts your data to hide what you are doing and your location from others.

Wi-Fi A means of connecting to the internet over the air. Also known as wireless.

Index

D

[Deleting your account](#)

G

[Glossary](#)

[Google Services](#)

[Gmail](#)

[Drive](#)

[Docs](#)

[Sheets](#)

[Slides](#)

[Forms](#)

[Drawing](#)

H

[Hacked, What to do if you are](#)

[Back up access](#)

[Password change](#)

[Sent mail](#)

Setting up 2-step verification, *in* [Chapter 3](#), *in* [Chapter 7](#)

P

[Passwords](#)

[choosing passwords](#)

[changing password](#)

Phishing *see* [Phishing and scams](#)

[Phishing and scams](#)

[An email from you](#)

[Bad grammar and spelling](#)

[Bank emails](#)

[Sob story](#)

[Too good to be true](#)

[Unsubscribing](#)

[Vacation scam](#)

[Privacy](#)

[In-Private browsing](#)

R

[Recovery Information](#)

[Email](#)

[Phone](#)

[Codes](#)

S

Scams Phishing see [*Phishing and scams*](#)

Security

[Why protect](#)

[Security keys](#)

[Buying keys](#)

[Setting up your Google account to use your key](#)

[Using a Security key](#)

Security threats

[Free Wi-Fi](#)

[Insecure sites](#)

[Shared devices](#)

[Social Engineering](#)

[Birth date](#)

[Mother's Maiden name](#)

[Pet's name](#)

[Social Security number](#)

Spam see [*Phishing and scams*](#)

T

[Two-factor authentication](#)

[accessing after setup](#)

[backup access](#)

[using mobile device](#)

[security keys](#)

[setting up](#)

[verification codes using Android apps](#)

More from Lycan Books & Myrddin Publishing:

A Simpler Guide to Calibre by Ceri Clark

A Simpler Guide to Finding Free eBooks by Ceri Clark

A Simpler Guide to Gmail by Ceri Clark

A Simpler Guide to Google+ by Ceri Clark

A Simpler Guide to Online Security for Everyone by Ceri Clark

After Ilium - Seduction, betrayal, and foreign adventure by Stephen Swartz

Brawn Stroker's Dragula by Nicole Antonia Carro. When the Vampire Queens battle, who will win?

Charm City Chronicles: Ednor Scardens, The Body War, The Hurting Year & On Gabriel's Wings by Kathleen Barker. Young adult romance.

Children of the Elementi by Ceri Clark YA fantasy. Five children must discover their powers and unite to save their world.

Crown Phoenix Series: The Night Watchman Express, Devil's Kitchen, The Lamplighter's Special & South Sea Bubble – Steampunk fantasy by Alison DeLuca.

Dark Places by Shaun Allan: 13 stories. 13 poems. 13 doorways of the mind for the demons to enter through.

Darkness Rising: Chained, Quest, Secrets & Loss - Epic fantasy by Ross Kitson.

Email Management using Gmail by Ceri Clark

Emeline & the Mutants - a post-apocalyptic horror set in Australia with zombies and vampires by Rachel Tsoumbakos.

Heart Search Series: Lost & Found - Fate toys with mortals and immortals alike in this Paranormal Romance series by Carlie Cullen.

Hearts and Minds - Poetry of Love, Loss, and Life by Maria V.A. Johnson.

Hired by a Demon - paranormal fantasy by Gypsy Madden.

Land Of Nod Trilogy: The Artifact and The Prophet - Sci-fi adventure by Gary Hoover.

Sax and the Suburb by Marilyn Rucker. Why is someone killing the community band geeks of Richland, Texas?

Silent No More by Krista Hatch. Trapped in 1942 Munich by a freak twist in time, two strangers must navigate their way to safety with only each other and the help of a group of university kids hell-bent on taking down Adolf Hitler and the entire Third Reich.

Sin: Horror and humor by Shaun Allan. People die around Sin. He doesn't like it and there's nothing he can do about it. But someone else knows, and Sin has to stop them... and himself.

Sons of Roland - A Rock Odyssey by Nicole Carro.

Tales from the Dreamtime: a novella of 3 fairy tales, by Connie J. Jaspersen.

The Dream Land Trilogy - Interdimensional intrigue and alien romance by Stephen Swartz.

The Infinity Bridge: A Sci-fi steampunk adventure set in modern day York, replete with androids, airships... and Merlin by Ross Kitson.

The Guardian Series: The Last Guardian and Burdens of a Saint by Joan Hazel - Paranormal Fantasy Romance. Without a Guardian, Haven will destroy itself.

The Ring of Lost Souls: A spooky paranormal gothic tale set in Australia by Rachel Tsoumbakos

Tower of Bones Series: Tower of Bones & Forbidden Road. Epic fantasy, by Connie J. Jasperson. The Gods are at war and the land of Neveyah is the battleground. Magic and destiny lie waiting in the Tower of Bones.

What the Heart Sees by Joan Hazel – Romance. Two brothers, one chance for happiness.

Yum - A yummy horror story. George Orwell meets George Romero! By Nicole Carro.

Copyright Information

A Simpler Guide to Online Security for Everyone: How to protect yourself and stay safe from fraud, scams and hackers with easy cyber security tips for your Gmail, Docs and other Google services

First Edition

Published by



Lycan Books (In association with Myrddin Publishing)

1 Monet Crescent,

Newport,

NP19 7PP

www.lycanbooks.com

Copyright © 2015 Ceri Clark

PRINT ISBN-10: 1-909236-11-X

PRINT ISBN-13: 978-1-909236-11-0

All rights reserved. No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form, or by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written permission of the author. Any person who does any unauthorized act in relation to this publication may be liable to criminal prosecution and civil claims for damages.

Limited Liability/Disclaimer of Warranty: While best efforts have been used in preparing this book, the author and publisher make no representations or warranties of any kind and assume no liabilities of any kind with respect to the accuracy or completeness of the contents and specifically disclaim any implied warranties of merchantability or fitness of use for a particular purpose. Neither the author nor the publisher shall be held liable or responsible to any person or entity with respect to any loss or incidental or consequential damages caused, or alleged to have been caused, directly or indirectly without limitations, by the information or programs contained herein. Furthermore readers should be aware that internet sites listed in this work may have changed or disappeared from

when this work was written to when it will be read. This work is sold with the understanding that the advice given herein may not be suitable for every situation.

Trademarks: Where trademarks are used in this book this infers no endorsement or any other affiliation with this book. Any trademarks used in this book are solely used for editorial purposes.

© 2015 Cover & Interior Design: Lycan Books

Don't miss out!

Click the button below and you can sign up to receive emails whenever Ceri Clark publishes a new book. There's no charge and no obligation.

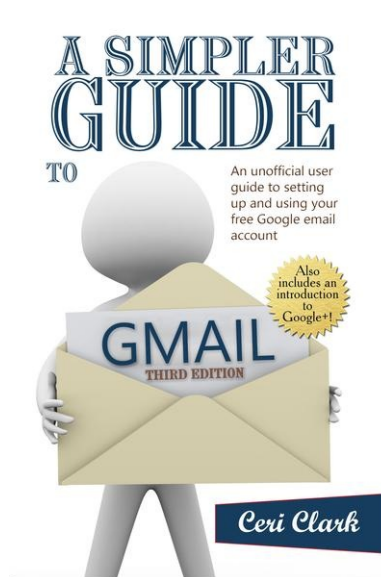
Sign Me Up!

<http://books2read.com/r/B-A-CKIB-OCWH>



Connecting independent readers to independent writers.

Did you love *A Simpler Guide to Online Security for Everyone: How to protect yourself and stay safe from fraud, scams and hackers with easy cyber security tips for your Gmail, Docs and other Google services?* Then you should read *A Simpler Guide to Gmail: An unofficial user guide to setting up and using your free Google email account. Third Edition* by Ceri Clark!



Gmail help for everyone!

Are you looking for a free email provider but you are not sure where to start? Do you use Gmail already but want tips on how to use it more effectively? Maybe you want to organize your emails better? Even if you just feel you are spending too much time on your email, then this guide for your Google mail account is for you!

Whether you call it Googlemail or Gmail, you are a Gmail ninja or a beginner, *A Simpler Guide to Gmail* is a complete illustrated user guide to setting up and using the free email service. Packed full of tips and information, this manual contains information on:

1. Why it is the best email solution for you, (Gmail is accessible from anywhere there is an Internet connection and as such is great for business and home use. Cloud computing is the future!)

2. Gmail sign in
3. Sending and receiving email
4. Google contacts, make networking a breeze with Gmail's address book
5. Email etiquette (Netiquette)
6. Email scams, spam and phishing - how to avoid them
7. Protecting your privacy
8. Helping to prevent hacking with the email security options that Google offers
9. Gmail setup for organizing your day
10. Understanding and using the settings (including filters) to organize your email inbox automatically to save you time (Email administration)
11. Using the Google mail app
12. Discovering and using Google+ and much more...

From the basics of setting up a Gmail login, your email address book, email organization to delving into the settings, *A Simpler Guide to Gmail* is a comprehensive consumer guide to the 'whys', 'hows' and 'whats' of getting the most out of a Google free email account. Take a look now to learn more of what Gmail can offer you.

Also by Ceri Clark

Elerian Chronicles
[Children of the Elementi](#)

Simpler Guides

[Email Management Using Gmail: Getting Things Done by Decluttering and Organizing your Inbox with email Organization Tips for Business and Home](#)
[A Simpler Guide to Gmail: An unofficial user guide to setting up and using your free Google email account. Third Edition](#)
[A Simpler Guide to Google+: An unofficial user guide to setting up and using the Google Plus social network](#)
[A Simpler Guide to Calibre: How to organize, edit and convert your eBooks using free software for readers, writers, students and researchers for any eReader](#)
[A Simpler Guide to Online Security for Everyone: How to protect yourself and stay safe from fraud, scams and hackers with easy cyber security tips for your Gmail, Docs and other Google services](#)