HOW GOOGLE HELPS KEEP THE BAD GUYS OUT

This information can be found at the Google Safety Center located at: https://www.google.com/safetycenter/everyone/cybercrime/

Avoid scams

No, you probably haven't won the lottery. You can't make that much working from home. And that deal really might be too good to be true.

The web can be a great place, but not everyone online has good intentions. Here are three simple ways to avoid scammers and stay safe on the web:

Beware of strangers bearing gifts

A message is probably up to no good if it congratulates you for being a website's millionth visitor, offers a tablet computer or other prize in exchange for completing a survey or promotes quick and easy ways to make money or get a job ("get rich quick working from your home in just two hours a day!"). If someone tells you you're a winner and asks you to fill out a form with your personal information don't be tempted to start filling it out. Even if you don't hit the "submit" button, you might still be sending your information to scammers if you start putting your data into their forms.

If you see a message from someone you know that doesn't seem like them, their account may have been compromised by a cybercriminal who is trying to get money or information from you – so be careful how you respond. Common tactics include asking you to urgently send them money, claiming to be stranded in another country or saying that their phone has been stolen so that they cannot be called. The message may also tell you to click on a link to see a picture, article or video, which actually leads you to a site that might steal your information – so think before you click!

Do your research

When shopping online, research the seller and be wary of suspiciously low prices just like you would if you were buying something at a local store. Scrutinize online deals that seem too good to be true. No one wants to get tricked into buying fake goods. People who promise normally non-discounted expensive products or services for free or at 90% off likely have malicious intent. If you use Gmail, you may see a warning across the top of your screen if you're looking at an email their system says might be a scam – if you see this warning, think twice before responding to that email.

Watch out for scams using the Google brand. Google does not run a lottery. They do not charge training fees for new employees – if you receive an email saying you have been hired by Google but have to pay a training fee before you can start, it is a scam. Watch out for people claiming to sell cars using Google Wallet.

When in doubt, play it safe

Do you just have a bad feeling about an ad or an offer? Trust your gut! Only click on ads or buy products from sites that are safe, reviewed, and trusted.

Many online shopping platforms have trusted merchants/sellers programs. These sellers typically have a visible stamp of approval on their profiles. Make sure that the stamp or certificate is legitimate by reviewing the shopping platforms' guidelines. If the platform doesn't offer a similar program, take a look at the number of reviews and the quality of reviews on the seller.

Google's extension Web of Trust can help you determine if a website is trustworthy.

Additional help

Several organizations may help you report and resolve any complaints: The Better Business Bureau and the National Consumers League both offer information. The Federal Trade Commission (FTC) handles complaints about deceptive or unfair business practices. To file a complaint, visit: www.ftc.gov/ftc/contact.shtm
You may wish to file a report with the appropriate authorities and/or your regional fraud reporting center — such as the Internet Crime Complaint Center (www.ic3.gov) which is a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center.

If your complaint is against a company in a foreign country, you may be able to report complaints at: www.econsumer.gov

Video: https://www.youtube.com/watch?v=3vcLyvoKYZc

How Google helps protect you from scams and personal fraud

Just like in the offline world, there are con artists and fraudsters on the Internet. Google takes a number of steps to help keep you from getting scammed.

Banning bad ads (and bad advertisers)

Google has very clear policies about who can show ads through Google's tools. They designed their ads policies with user safety and trust in mind. For example, they don't allow ads for malicious downloads, counterfeit goods or ads with unclear billing practices. And if they find an ad scam, they don't just ban the ad – they ban the advertiser from ever working with Google again.

Being clear about costs

One way that online criminals make money is by using someone's computer or phone to do something that costs that person money, and gives money to the criminal. For example, one scheme is to create an app that can make someone's phone send text messages or call a paid phone chat line, which then charges that person money, which is collected by the scammer.

On phones powered by Android, you can see what an app will request to do with your phone by looking at the description in Google Play that says "permissions." Look at this information before you download an app to help decide whether you want to get it or not. For example, if you're getting ready to download a new ringtone app, you can see if that app may make phone calls on your behalf. If you decide that sounds suspicious, you can decide not to install the app.

For more recent Android devices, Google will let you know if an app tries to send SMS to a telephone number that might cause you additional charges. You can then choose whether to allow the application to send the message or block it.

Video: https://www.youtube.com/watch?v=4VewFkix7qg

Prevent identity theft

Just like burglars and thieves, cyber criminals have many different ways to steal personal information and money. Just as you wouldn't give a burglar the key to your house, make sure to protect yourself from fraud and online identity theft. Know the common tricks that criminals employ to help you protect yourself from online fraud and identity theft. Here are a few simple tips.

Don't reply if you see a suspicious email, instant message or webpage asking for your personal or financial information

Always be wary of any messages or sites that ask for your personal information, or messages that refer you to an unfamiliar web page asking for any of the following details:

- Usernames
- Passwords
- Social Security numbers
- Bank account numbers

- PINs (Personal Identification Numbers)
- Full credit card numbers
- Your mother’s maiden name
- Your birthday

Don’t fill out any forms or sign-in screens that might be linked to from those messages. If someone suspicious asks you to fill out a form with your personal information don’t be tempted to start filling it out. Even if you don’t hit the “submit” button, you might still be sending your information to identity thieves if you start putting your data into their forms.

If you see a message from someone you know that doesn’t seem like them, their account may have been compromised by a cybercriminal who is trying to get money or information from you – so be careful how you respond. Common tactics include asking you to urgently send them money, claiming to be stranded in another country or saying that their phone has been stolen so they cannot be called. The message may also tell you to click on a link to see a picture, article or video, which actually leads you to a site that might steal your information – so think before you click!

Never enter your password if you’ve arrived at a site by following a link in an email or chat that you don’t trust

Even if you think it’s a site that you trust, like your bank, it’s better to go directly to the site by using a bookmark or typing in the site’s address directly into the browser.

Don’t send your password via email, and don’t share it with others

Your passwords are the key to your accounts and services online, and just like in your offline life, you should be careful who you give your keys to. Legitimate sites and services won’t ask you to send them your passwords via email, so don’t respond if you get requests for your passwords to online sites.

Because your passwords are so important, you should think carefully before deciding to share them with others – even friends and family. When you share your passwords, there is a greater risk that someone may misuse your accounts by accessing information you don’t want them to have or using the account in ways you don’t approve. For example, if you share your email password with someone, that person might read your personal emails, try to use your email account to access other online services you might use, like banking or social sites, or use your account to impersonate you. Finally, when you share your password with someone, you will have to rely on them to keep it secure; they may share it with others on purpose or by accident.

Pay close attention when asked to sign in online

Check for signals about your connection with the website.

First, look at the address bar in your browser to see if the URL looks real. You should also check to see if the web address begins with https:// – which signals that your connection to the website is encrypted and more resistant to snooping or tampering. Some browsers also include a padlock icon in the address bar beside https:// to indicate more clearly that your connection is encrypted and you are more securely connected.

Report suspicious emails and scams

Most email providers, including Gmail, allow you to do this. Reporting a suspicious message in Gmail will help block that user from sending you more emails and help our abuse team stop similar attacks.

Video: https://www.youtube.com/watch?v=X4Dq0XYkwH0

How Google helps you combat identity theft

Google uses a variety of technologies to help protect you from online identity theft and make sure your Google Account stays safe and secure.

2-step verification

To bring even stronger levels of protection to your Google Account, they offer 2-step verification to users. This tool adds an extra layer of security by requiring not just a password, but also a verification code to sign in to a Google Account. Even if your password is cracked, guessed, or otherwise stolen, an attacker can't sign in to your account without entering the verification code they will send to your mobile phone. Google offers 2-step verification in more than 50 languages and 175 countries.

Encryption

Google takes many steps to keep your personal information safe from attackers and snoops. By default, they encrypt the Gmail connection between your computer and Google – this helps protects your Google activity from being snooped on by others. They also make this protection, known as session-wide SSL encryption, the default when you're signed into Google Drive and many other services.

Suspicious account activity warnings

Google has alerted a number of users when it looked like something unusual was going on with their Google Account – for example, logins appearing to come from one country and occurring shortly after a login from another country. These users were shown a warning message in their Gmail inbox about this unusual access. Google also occasionally make users change their passwords if they have reason to believe their account has been compromised.

Email authentication

To help fight abuse and keep spam out of your inbox, Gmail uses email authentication to determine if a message actually originated from the address from which it appears to be sent. All active Gmail users – and the people in contact with them – automatically receive protection against threats to their personal and financial information.

Spam protection

Gmail protects you from spam and harmful emails. Gmail processes billions of messages every day and has an outstanding track record when it comes to protecting users from spam – less than 1% of all the spam in Gmail ends up reaching someone's inbox. When a spammer sends a new type of junk mail, Google's systems often identify and block it from Google accounts within minutes. This makes it less likely that spammy messages that might hurt your computer or try to steal your personal information will be able to do so.

Video: https://www.youtube.com/watch?v=1ktecMB1_Ws

Keep your device clean

Is your device running a bit slower than usual? Maybe random screens are popping up? Does your bank account have unknown charges on it?

These are some signs that your device might be infected with malware – malicious software designed to harm your device or network.

Here are simple ways to help protect yourself:

Keep your browser and operating system up to date

Most operating systems and software will notify you when it's time to upgrade – don't ignore these messages and update as soon as you can. Old versions of software can sometimes have security problems that criminals can use to more easily get to your data. Google's Chrome browser automatically updates to the latest version every time you start it up, so you can get the most up-to-date security protection without any extra work.

Always keep an eye on what you click and download, including music, movies, files, browser plug-ins or add-ons

Be wary of pop-up windows that ask you to download software or that offer to fix your computer. Often these pop-ups will claim that your computer has been infected and that their download can fix it – don't believe them. Close the window and make sure you don't click inside the pop-up window. Do not open files of unknown types, or if you see unfamiliar browser prompts or warnings asking you to open a file. Sometimes malware may prevent you from leaving a page if you land on it, for example by repeatedly opening a download prompt. If this happens, use your computer's task manager or activity monitor to close your browser. To get to the task manager, hold down the CTL, ALT and Delete button all at the same time.

When in doubt, use trusted bookmarks for important sites, use your search engine to navigate to the site or type the site address directly into your browser. You should also check to see if the web address begins with https:// – which signals that your connection to the website is encrypted and more resistant to snooping or tampering.

When you do install software, make sure you're getting the software from a trusted source

Some programs bundle malware as part of their installation process. Before you start a download, there are a few simple steps you can take to help reduce your risk of downloading malware along with the software you want.

Check the reputation of the store – is it an authoritative source, like your phone or browser's built-in app store, or the developer's website, as opposed to an unfamiliar third-party download site? You can also check the reputation of the developer by looking at what others have said about them in the past. Check for online review or comments about that particular download. If you see that many people didn't like it or had a bad experience, you might not want to download it yourself.

If you notice something suspicious after your download – such as significant computer slowness, unexpected pop-ups or messages, or unfamiliar billing charges – uninstall the software immediately and make sure your anti-virus is running and up-to-date.

Many browsers will warn you if you try to go to a website that is suspected of hosting malware. If you get a warning that a site you want to visit may not be safe, look at the URL and think carefully about whether you want to visit the site or not. Even if you have visited the site before, criminals may have compromised the site since the last time you visited, so it may not be safe to go to until the site's owners have cleaned up their site.

If your computer is infected with malware, remove it as soon as you can

One way to clean your computer is to scan it with at least one, and ideally a few, high-quality antivirus products.

- AVG
- AVIRA
- BitDefender
- ESET Smart Security
- F-Secure
- G DATA
- Kaspersky Lab Internet Security
- McAfee

- MacScan (for Mac users)
- Microsoft Security Essentials
- Norton Internet Security
- TrendMicro
- Malwarebytes

Video: https://www.youtube.com/watch?v=uJRqZTNMCMo

How Google helps you keep your computer and device clean

While some criminals might be after your information, like your bank account details, email inbox or online passwords, others may be looking to take control of your device – your computer, tablet or phone.

Criminals can then use your device to find other devices that they can control. They often use armies of computers to knock websites offline or breach their security systems.

One of the top ways that criminals can take control of your computer is by installing malicious software, or malware. You can help protect your computer from malware, but Google also works hard to help protect you too, with hundreds of security experts working around the clock to help ensure your data and devices are secure.

Helping you avoid malware

Just like Google searches the web for sites with the best answers to your questions, we also look for sites that appear to be harmful to users or have malware on them. Every day Google identifies and flags more than 10,000 of those unsafe sites, and they show warnings on as many as 14 million Google Search results and 300,000 downloads, telling users that there might be something suspicious going on behind a particular website or link.

Google also uses the same technology to help identify if someone is sending you a message in Gmail that might be harmful or have malware, and to warn you if you try to download something from a website that might look like a ringtone or a PDF, but secretly contains code that could harm your computer.

Even if you do go to a page with malware, Google's engineers have built additional defenses into the Chrome browser that help prevent malware from installing itself on your computer, and minimize the impact of malware on your computer.

Helping you stay up to date

One way that criminals sometimes gain access to your computer is by looking for known security problems in old versions of software that is running on your device. They know that many people don't always update to the latest version of their computer software and programs, which has the best security protections. Google knows this too, which is why we built the Chrome browser to auto-update to the latest version every time you start it up, so you can get up-to-date security protection without any extra work.

Chrome sometimes has to work with other software, called plug-ins, to do things like show pictures or video properly. These plug-ins can also be a way for criminals to gain control of your computer. If Chrome detects an out-of-date plug-in with a security problem, it will block that plug-in until you have the most up-to-date and secure version and show you a message telling you the plug-in needs to be updated.

Helping you keep your mobile device safe

Smartphones running Google's Android software have similar protections in place to reduce the risk of damage.

Android also requires that every app in the Google Play store list what kind of information the app wants to collect or access from your device, so you can decide whether you trust the app or not. Google also automatically scans Google Play to block and remove harmful apps, and for some Android phones, the Google Application Verifying Service will check for potentially harmful applications no matter where you are installing them from. So, if you install applications from unknown sources like the web or a third party app store, this free service will provide you with another layer of security.