Google News Initiative

5 LESSONS 44 MIN TOTAL

Safety and Security

This vital course teaches you how to protect yourself and your news organization from hacking, digital attacks and censorship.

Tools Used:
Project Shield, 2-Step Verification, Password Alert

Google News Initiative

LESSON 01

Project Shield: Defend against digital censorship

A free tool to protect your site from Distributed Denial of Service (DDoS) attacks.

Lesson overview

Protecting websites from digital attacks.

Every day, independent news sites around the world are taken offline and effectively silenced by digital attacks. During controversial events such as elections, civil unrest or conflict, the threat level increases even more.

Following the 2015 Charlie Hebdo attacks in Paris, an unprecedented surge in Distributed Denial of Service (DDoS) attacks targeted as many as 19,000 French websites. And the problem has grown far worse since then. The year 2017 saw attacks worsen, both in volume and sophistication. In 2018, a DDoS attack knocked a Tennessee county election website offline during voting. Even GitHub has been taken down by one.

Project Shield is a free tool that uses Google's technology to protect news publishers from this growing daily threat.

1 What is a “DDoS” attack?

2 A growing threat to news publishers.

3 Project Shield protects your site for free.

4 Who can apply for Project Shield?

5 How to apply for Project Shield.

For more Safety and Security lessons, visit:

newsinitiative.withgoogle.com/training/course/safety-and-secruity

What is a “DDoS” attack?

SINGLE STEP

A DDoS attack occurs when someone exploits thousands or even millions of computers and tricks them into visiting a specific website at the same time. The resulting flood of “junk” traffic often overwhelms servers and crashes the website, taking it offline. The damage doesn’t stop there. Attempting to fight off or recover from a DDoS attack can be devastatingly expensive and time-consuming.

To make matters worse, DDoS is no longer the exclusive purview of elite computer hackers; nearly anyone with an Internet connection can launch one for as little as $5 (U.S.). Today, even an average-size attack can take most sites offline.

To better understand DDoS attacks, watch this video.

A growing threat to news publishers.

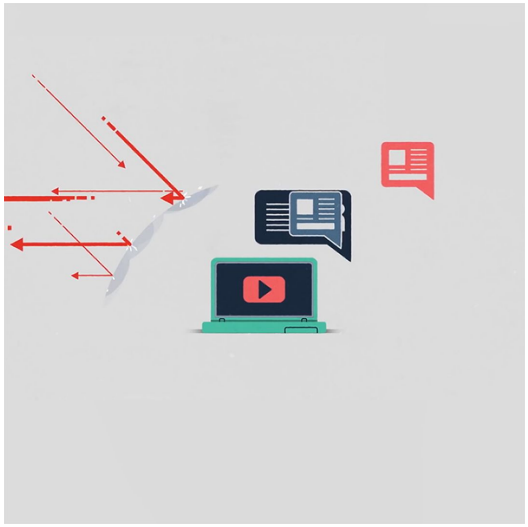
SINGLE STEP

DDoS attacks are growing increasingly common and complex. According to Arbor Networks, the 10 most attacked countries saw increases as high as 56% from 2016. In the U.S. Arbor estimates there were 153,083 attacks per month in 2017. According to Neustar, the odds of getting hit are one in two, with repeat attacks as common as 80%. And no one is immune: even some of the world's largest publishers have been taken down by DDoS.

To see where DDoS attacks are happening right now, check out Digital Attack Map, a live data visualization that surfaces anonymous attack traffic data so you can explore historic trends and find reports of outages happening on any given day.

Project Shield protects your site for free.

SINGLE STEP



These alarming statistics point to the need for robust DDoS protection -- which can be prohibitively complicated and expensive. Project Shield is a free tool that leverages Google infrastructure to protect news publishers, no matter how many attacks they experience.

Project Shield is a “reverse proxy” that uses Google’s own defenses and network capacity to protect news sites. This provides a “shield” against would-be attackers by filtering out malicious traffic. It also caches some site elements to lighten the load on your own servers, which can improve site performance and reduce your bandwidth costs.

Who can apply for Project Shield?

SINGLE STEP

There are four categories of sites eligible for inclusion under Project Shield:

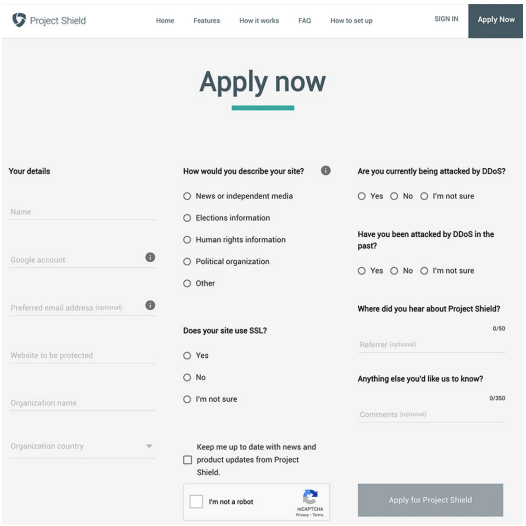
News: You regularly publish timely content with attribution to keep readers informed on important information.

Human rights: Nonprofits dedicated to one of the UN charters of human rights.

Elections: Information on polling locations, vote monitoring, and election results. You can review our content and quality guidelines to see whether your site is likely to qualify.

Political organizations: Certain countries and political organizations may be eligible, subject to local laws. To learn more, click here.

Citizen journalism sites may apply but will be evaluated on a case-by-case basis.



How to apply for Project Shield.

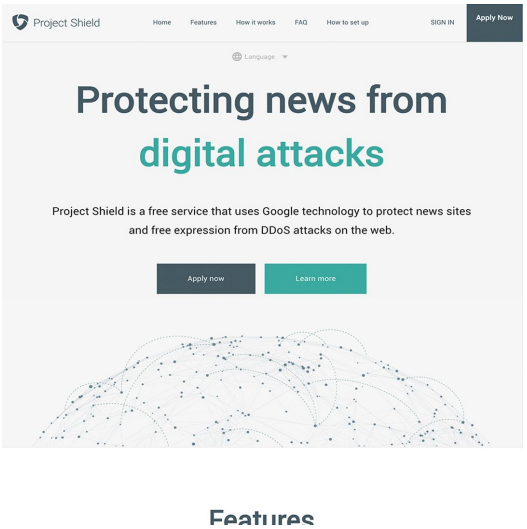
Go to g.co/shield and follow steps below.

Once your site is approved, you'll receive instructions on how to route your traffic through Project Shield. This simple setup process takes just a few minutes, and then you'll be protected from DDoS attacks.

To learn more, check out our FAQs.

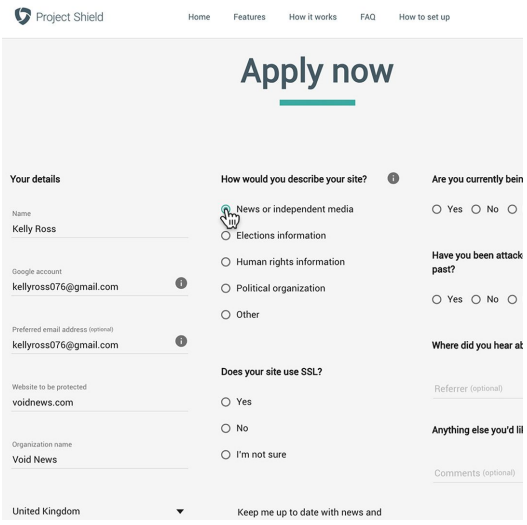
STEP 1 OF 2

Click "Apply now"



STEP 2 OF 2

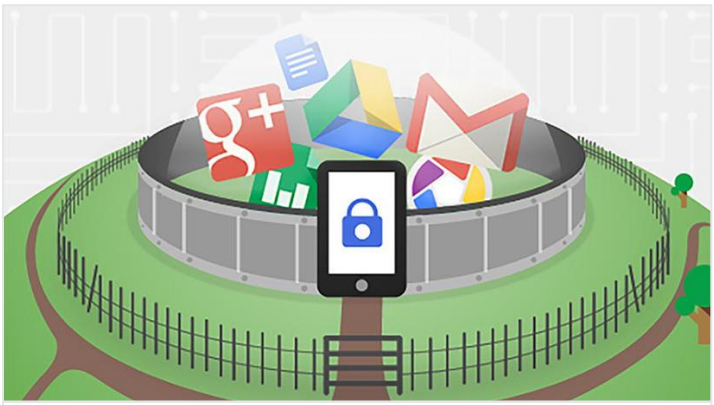
Fill in form



Congratulations!

You completed “Project Shield: Defend against digital censorship.”

To continue building your digital journalism skills and work toward Google News Initiative certification, go to our Training Center website and take another lesson:



14 min estimated time

2-Step Verification: Stronger security for your Google account

Add an extra layer of protection beyond your password.

For more Safety and Security lessons, visit:

newsinitiative.withgoogle.com/training/course/safety-and-secruity

Google News Initiative

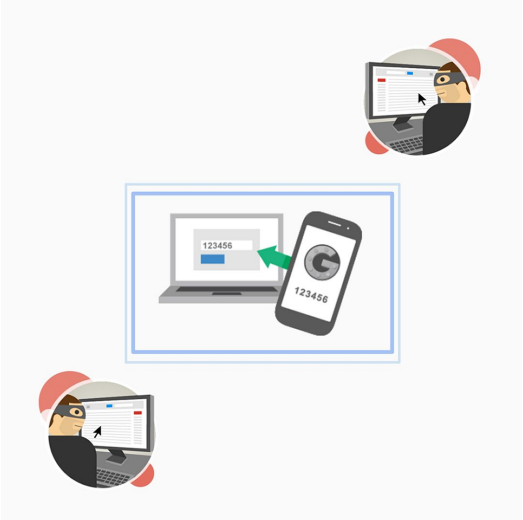
LESSON 02

2-Step Verification: Stronger security for your Google account

Add an extra layer of protection beyond your password.

Lesson overview

Passwords are only the first line of defense.



A strong password is crucial to account security, but it's not impassable. Many common actions leave you vulnerable; including using the same password on more than one site, downloading software, or clicking on links in email messages. Once your password is stolen, a hacker can access your email, contacts, photos and documents. They can pretend to be you and send out harmful emails, lock you out of your account, delete all of your data and/or reset passwords on things like your banking accounts.

Since journalists are frequent hacking targets, it's important to secure your account with the best tools available. Google's 2-Step Verification can help keep hackers out, even if they've acquired your password.

1. 2-Step Verification adds an extra layer of security.
2. How to set up phone-based 2-Step Verification.
3. Completing installation.
4. What is a Security Key?
5. Set up your Security Key(s).
6. Choose a backup security method.

For more Safety and Security lessons, visit:

newsinitiative.withgoogle.com/training/course/safety-and-secruity

2-Step Verification adds an extra layer of security.

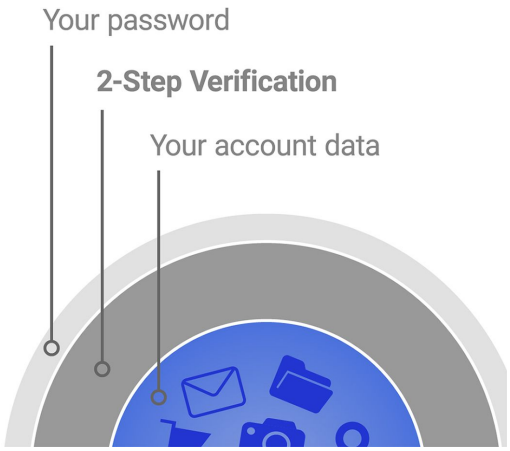
SINGLE STEP

When you use 2-Step Verification, signing in to your account will work a little differently.

1. You'll enter your password. Whenever you sign in to Google, you'll enter your password as usual.

2. You'll be asked for a second step. Then, you'll need to enter a code, which you'll receive on your phone via text, voice call, or our mobile app. Or, if you have a Security Key, you will insert it into your computer's USB port.

With 2-Step Verification, even if a bad guy hacks through your password layer, he would still need your phone or Security Key to get into your account.

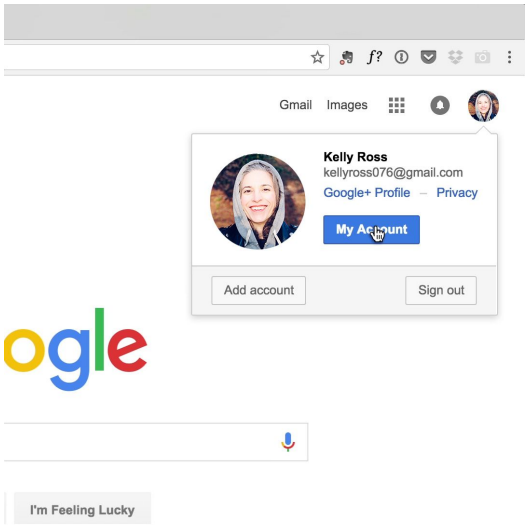


How to set up phone-based 2-Step Verification.

First, we'll show you how to use phone-based 2-Step Verification, so you can protect your account right away. We'll cover Security Keys later in the lesson.

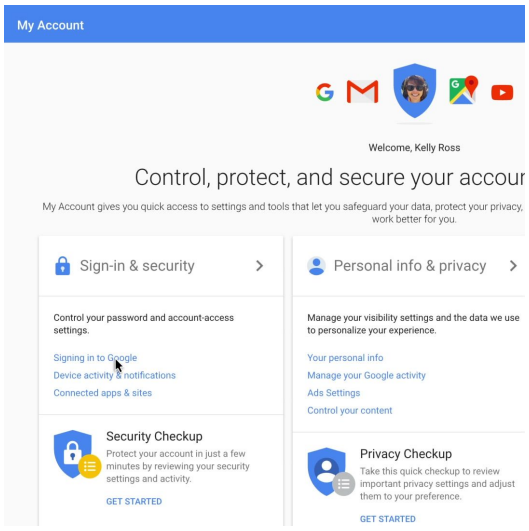
STEP 1 OF 4

To begin installation, log in to your Google account as you normally would and click **My Account**.



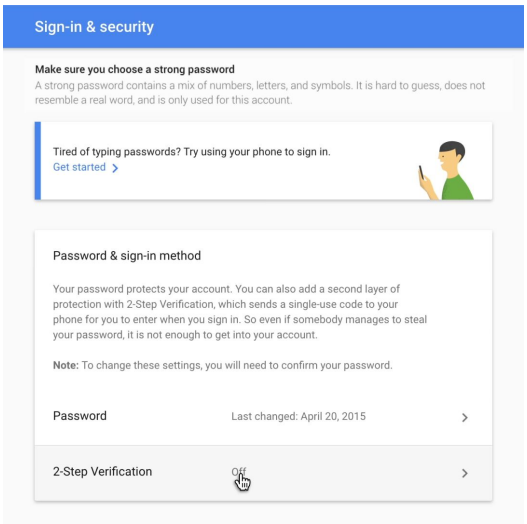
STEP 2 OF 4

Select **Sign In and Security** > **Signing in to Google**.



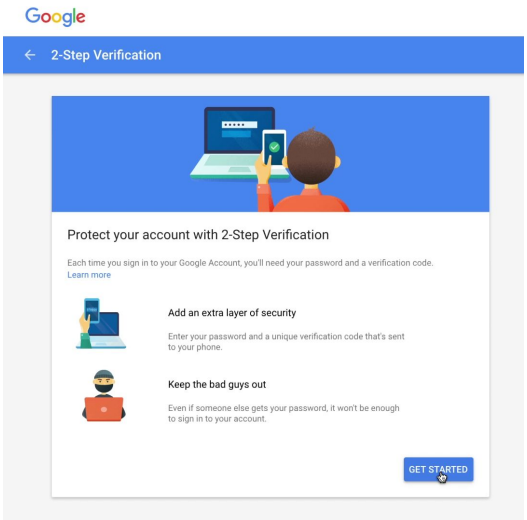
STEP 3 OF 4

Under **Password & sign-in method**, you can see that it says **2-Step Verification: Off**.



STEP 4 OF 4

Select that link, then click **Get Started** to begin.

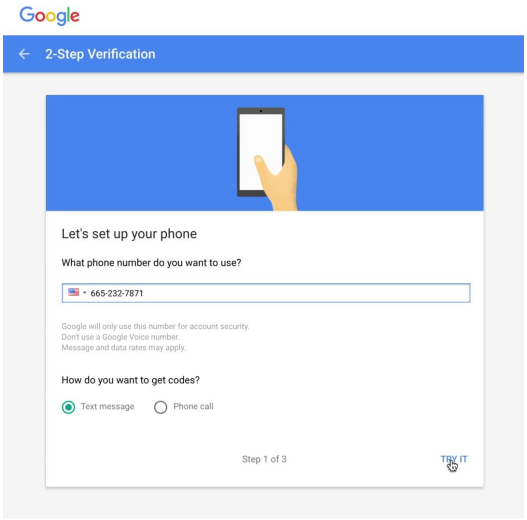


Completing installation.

You should now be looking at your Google sign-in page. Enter your password again to get to the next page.

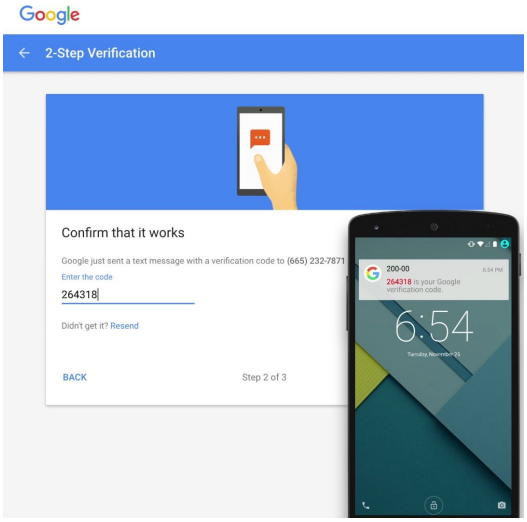
STEP 1 OF 5

Now, you can enter a phone number to receive verification details and choose whether you want the code via text or voice call.



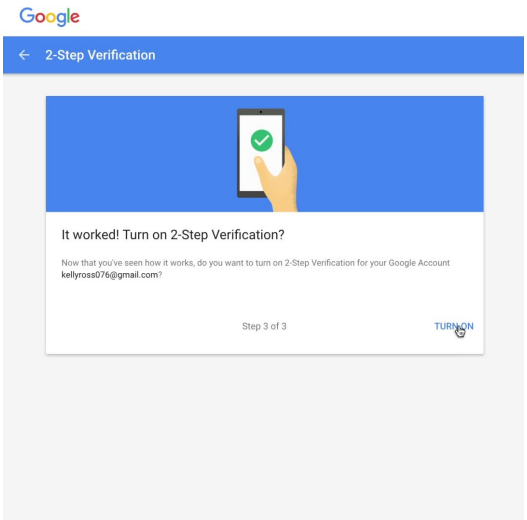
STEP 2 OF 5

You'll get a code delivered to confirm that the system is working.



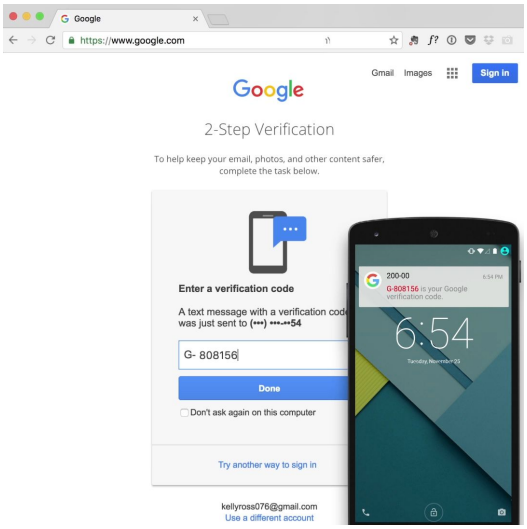
STEP 3 OF 5

Next, you'll confirm that you want to turn on 2-Step Verification.



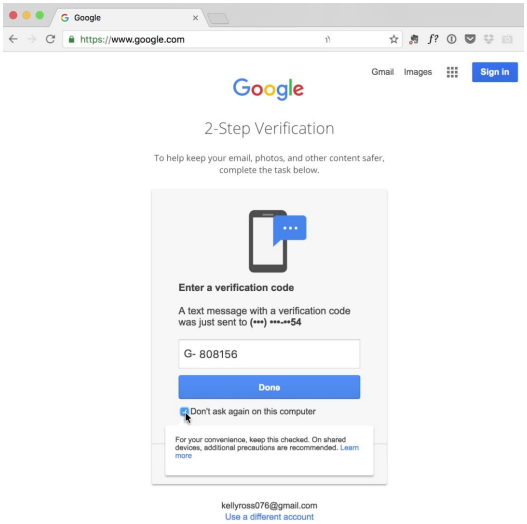
STEP 4 OF 5

Once it's enabled, the next time you sign in, Google will ask you to enter a passcode to verify your identity.



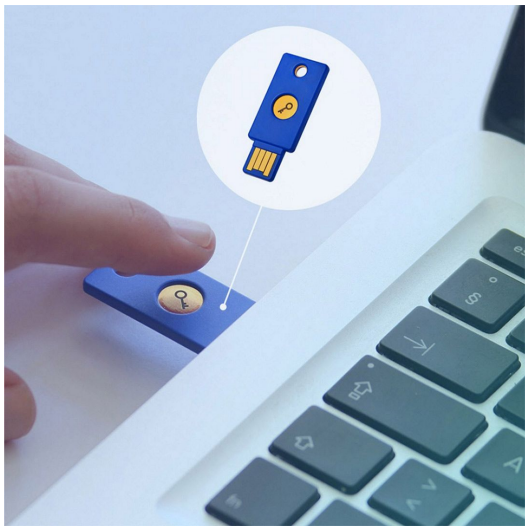
STEP 5 OF 5

You can ask Google to trust your machine by checking **Don't ask again**. From then on, that computer will ask only for a password and not a verification code during sign-in.



What is a Security Key?

SINGLE STEP



While you may be familiar with verification codes sent via phone, fewer people know about Security Keys. A Security Key is a small, physical device used for signing in that plugs into your computer's USB port. Advantages include:

Better protection against phishing. Even with the phone method of 2-Step Verification, you are still vulnerable to sophisticated attackers who can forge Google lookalike sites that ask for your verification codes. A Security Key uses cryptography instead of verification codes and automatically works only with the website it's supposed to work with.

No mobile connection or batteries needed. Security Key works without a data connection, and you can carry it wherever you go on a keychain or in your wallet.

You can choose either a phone or Security Key as your primary verification method.

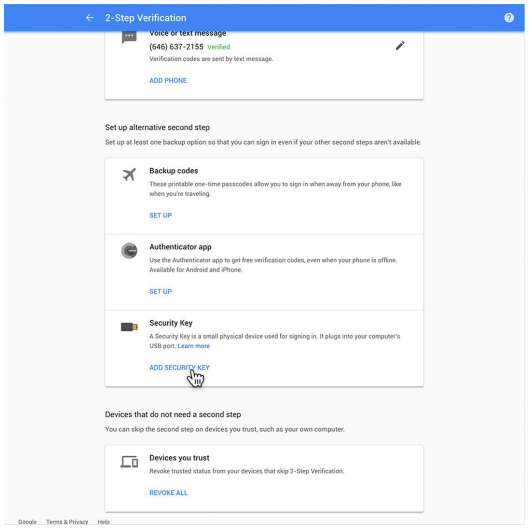
Set up your Security Key(s).

You can easily purchase a Security Key online -- just be sure you choose a device that is compliant with the open standard called “FIDO Universal 2nd Factor (U2F).”

Before you can use your Security Key, you’ll need to register it to your Google Account so that you can use it to sign in on any computer.

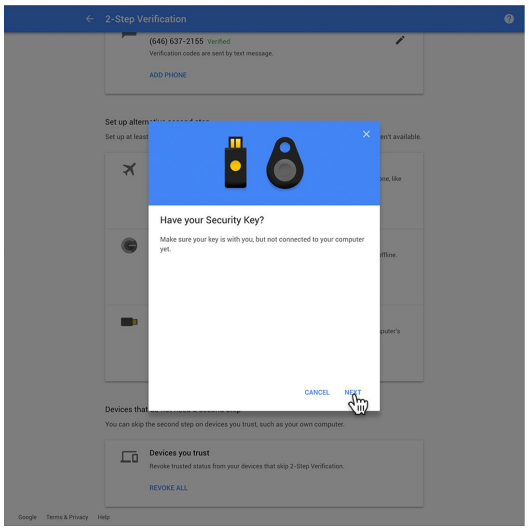
STEP 1 OF 3

In the 2-step verification section of your account, go to **Add a Security Key**.



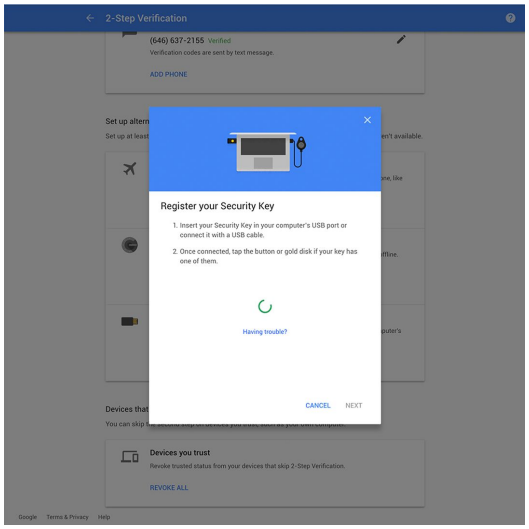
STEP 2 OF 3

To sign in, tap or insert the key when prompted. You won’t need to re-type codes from your phone.



STEP 3 OF 3

It’s a good idea to register more than one Security Key to your account, in case you lose one.

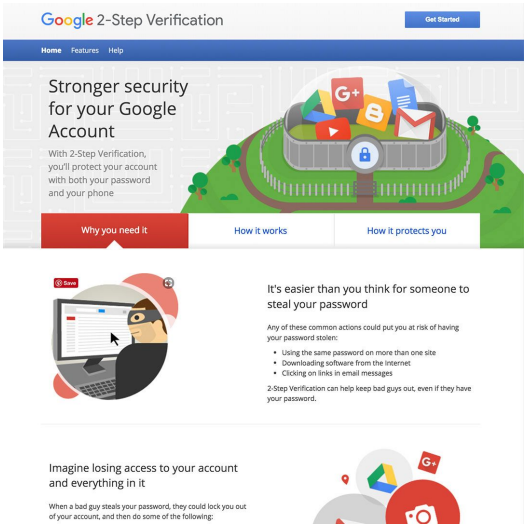


Choose a backup security method.

SINGLE STEP

No matter which primary verification method you use, you'll want to set up at least one backup option so that you can still sign in even if you don't have your phone or Security Key. No matter what you choose, you'll feel confident knowing your account is both secure and accessible when you need it.

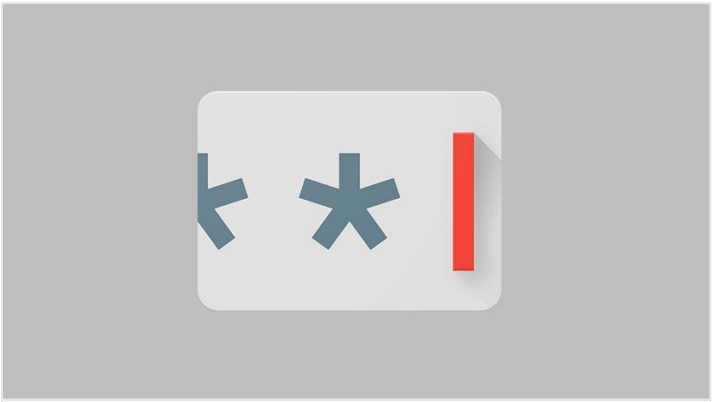
For more information, visit the 2-Step Verification site.



Congratulations!

You completed “2-Step Verification: Stronger security for your Google account.”

To continue building your digital journalism skills and work toward Google News Initiative certification, go to our Training Center website and take another lesson:



10 min estimated time

Password Alert: Protect yourself from password theft

This simple Chrome extension is your first line of defense.

For more Safety and Security lessons, visit:

newsinitiative.withgoogle.com/training/course/safety-and-secruity

Google News Initiative

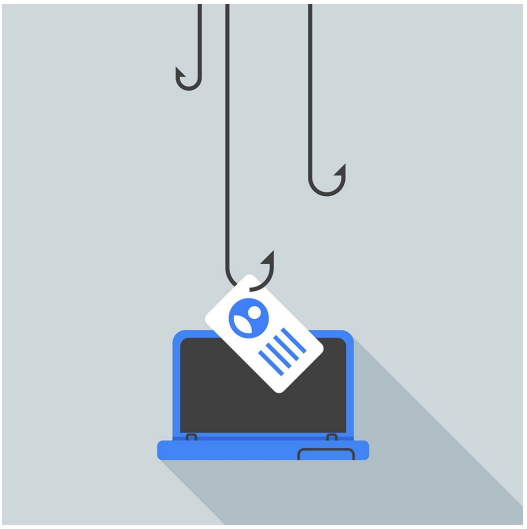
LESSON 03

Password Alert: Protect yourself from password theft

This simple Chrome extension is your first line of defense.

Lesson overview

Password thieves often target news media.



Every day, hundreds of millions of emails are sent with the intent of stealing passwords. Increasingly, these attacks target journalists: a 2014-2015 study by Newscycle Solutions found that 52% of news media companies were hacked or suffered a data breach -- and the most common type of attacks were phishing (59%).

In 2016, a wave of cyberattacks in the U.S. that breached high-profile targets including the Democratic National Committee, Colin Powell and Olympic gymnast Simone Biles, underscored the need for enhanced security.

1 The rise of fake login pages.

2 How Password Alert protects you.

3 Password Alert maintains your privacy.

4 How to install Password Alert.

For more Safety and Security lessons, visit:

newsinitiative.withgoogle.com/training/course/safety-and-secruity

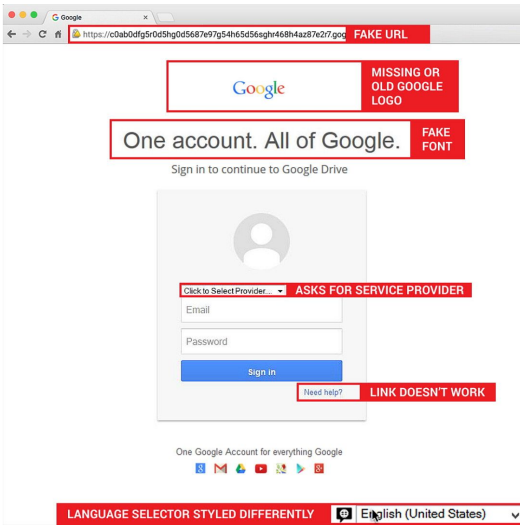
The rise of fake login pages.

SINGLE STEP

As phishing scams become more sophisticated, fake login pages can trick you into giving your password to an attacker -- without even knowing it. An action as simple as a typo can land you on one, with only subtle cues such as an outdated Google logo or font to tip you off that it's a forgery. That's how fake login pages successfully steal passwords 45% of the time.

Once your password has been stolen, the attacker may use your email account to harm you by gathering personal information or emailing others and pretending to be you. The consequences can be devastating; stolen data has even been used to put journalists in prison.

Password Alert lets you know if you've been targeted by this type of attack.

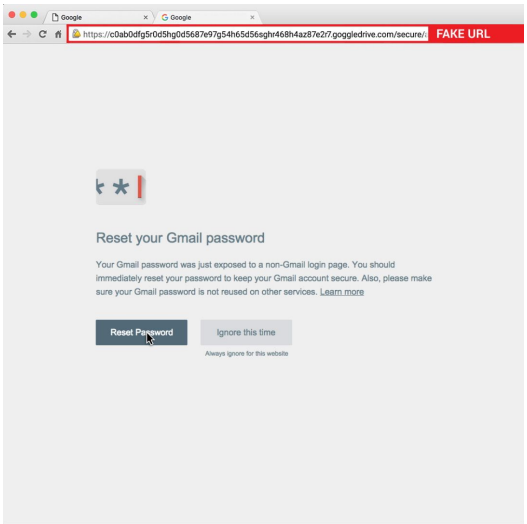


How Password Alert protects you.

SINGLE STEP

Created by Jigsaw and Google's Security Engineering and Google for Work teams, Password Alert works like a spellchecker, except that instead of looking for typos, it looks to see if you enter your Google account password any place other than your account sign-in page.

If it detects that you've mistakenly entered your password on the wrong site, it immediately alerts you and prompts you to change it. If you're positive that you're on a legitimate site, you can choose to ignore the alert and continue without changing your password.

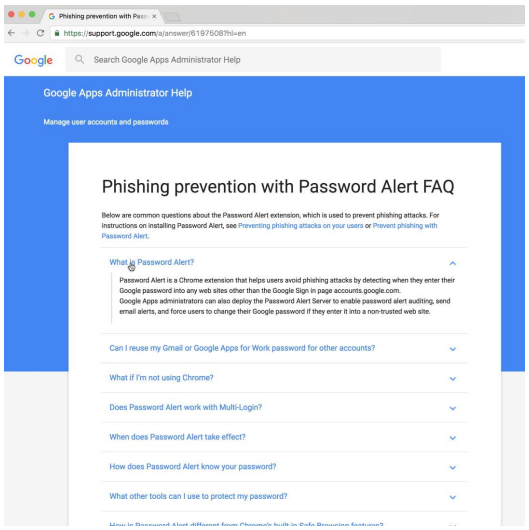


Password Alert maintains your privacy.

SINGLE STEP

Rest assured that Password Alert will never store your password or keystrokes. Using a technique called “hashing,” it knows if you typed your password without ever knowing what your password is.

To learn more about your privacy and Password Alert, read the FAQ on our support page.



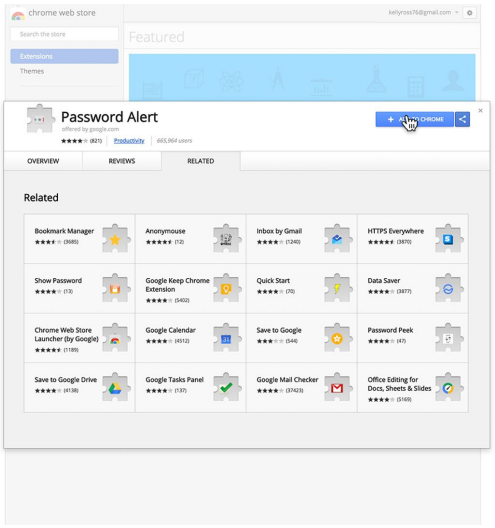
How to install Password Alert.

To install this safety tool, simply visit g.co/passwordalert, which takes you to the Chrome Webstore page where you can download Password Alert.

Once you've installed Password Alert, simply sign in to your Google account and it will automatically start working behind the scenes. To learn more about how Password Alert protects you online, visit the Jigsaw website.

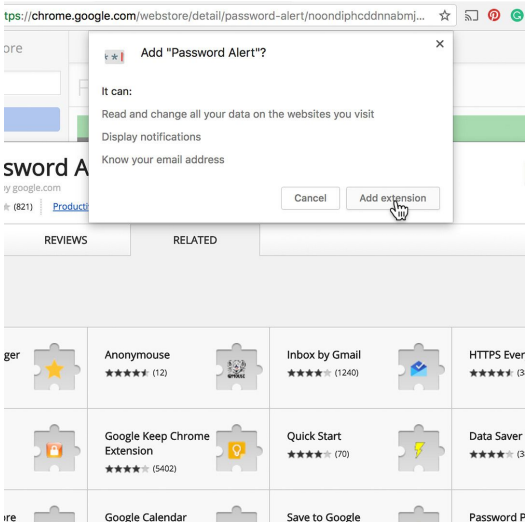
STEP 1 OF 2

Click on "Add to Chrome."



STEP 2 OF 2

Then click "Add extension" and Password Alert will install in your Chrome browser.



Congratulations!

You completed “2-Step Verification: Stronger security for your Google account.”

To continue building your digital journalism skills and work toward Google News Initiative certification, go to our Training Center website and take another lesson:

5 min estimated time

Advanced Protection Program: The strongest security for your Google account

Stronger security for your Google account.

For more Safety and Security lessons, visit:

newsinitiative.withgoogle.com/training/course/safety-and-secruity

Google News Initiative

LESSON 04

Advanced Protection Program: The strongest security for your Google account

Stronger security for your Google account.

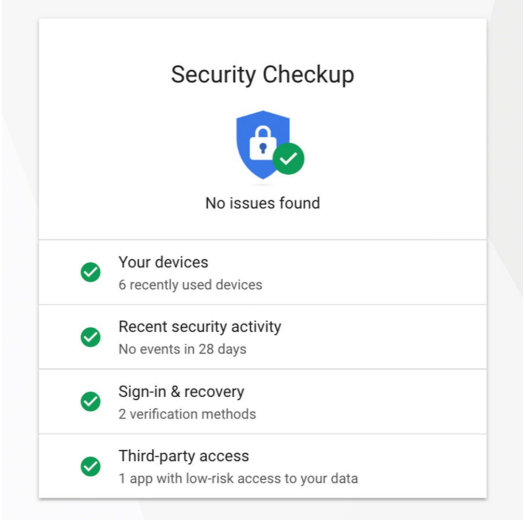
Lesson overview

Journalists face elevated risks online.

Safety and security online is important for everyone, but it's particularly crucial for journalists who need to consider the safety of their sources in addition to themselves.

Even the most careful and security-minded users can fall victim to sophisticated phishing scams. Reporters covering oppressive regimes or working in regions where freedom of the press is limited have been targeted by government-backed attackers. Entire news sites have been taken down by DDoS (Distributed Denial of Service) attacks. And journalists' data is increasingly at risk from cyber attacks.

Google's Advanced Protection Program was designed for journalists who face these elevated risks, and provides the extra layer of protection they may need.



1 Assess your level of threat.

2 Protect yourself with our strongest account security.

3 More resources for safety and security.

For more Safety and Security lessons, visit:

newsinitiative.withgoogle.com/training/course/safety-and-secruity

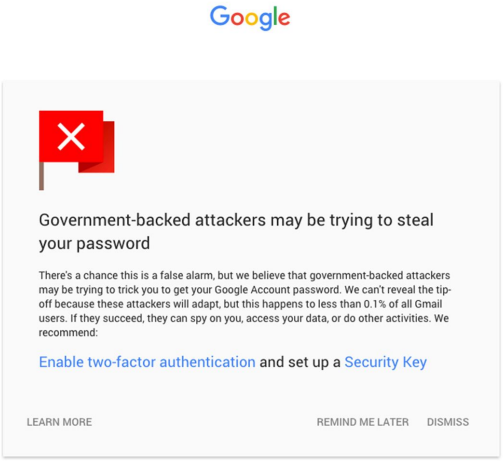
Assess your level of threat.

SINGLE STEP

First, run a security checkup on your google account. This is recommended for all users, but especially for journalists. Then, ask yourself the following questions:

- Do you work in a hostile climate?
- Do you have sources whose identities need to be protected?
- Do you get messages about government-backed attacks on Gmail?
- Do you see suspicious activities around your account? (for example, password recovery attempts not initiated by you)
- Would your work be viewed as controversial by some people?

If you answered “yes” to any of these questions, you would be a good fit for the Advanced Protection Program.



Protect yourself with our strongest account security.

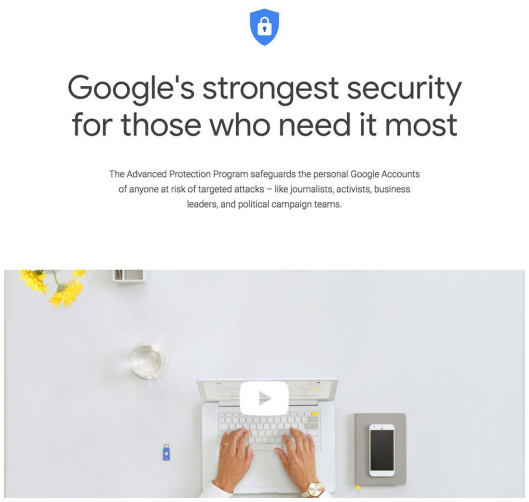
SINGLE STEP

The Advanced Protection Program is designed to safeguard the personal Google Accounts of those most at risk of targeted attacks.

Google Advanced Protection Program provides:

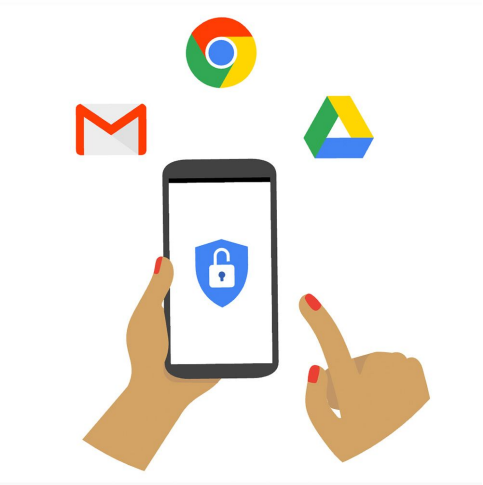
- The strongest defense against phishing
- Data protection against malicious and insecure applications
- Better vetting against fraudulent account recovery requests
- Deep scanning for incoming documents

To learn how to enroll, watch this helpful video.



More resources for safety and security.

SINGLE STEP



According to a recent study of more than 2,700 newsroom managers and journalists from 130 countries, at least half of those surveyed don't use any tools to protect their information online. We encourage journalists everywhere to take strong measures to improve their digital safety and security.

To learn more about protecting yourself online, visit the Advanced Protection Program website, read our Medium posts on digital security for journalists and watch our Advanced Security for Journalists Webinar.

Congratulations!

You completed “Advanced Protection Program: The strongest security for your Google account.”

To continue building your digital journalism skills and work toward Google News Initiative certification, go to our Training Center website and take another lesson.

For more Safety and Security lessons, visit:

newsinitiative.withgoogle.com/training/course/safety-and-secruity