Google

Cybersecurity challenges for Small and Medium Business

Introduction

Cybersecurity concerns are top of mind for small business owners. Small businesses are particularly vulnerable to cyberattacks, as they often have fewer resources and expertise to defend themselves. However, there are a number of steps that small businesses can take to improve their cybersecurity posture and protect themselves from cyber threats.

This guide will discuss some of the most important cybersecurity measures that small businesses can implement, as well as resources, tools, and support that Google provides to help them. With informed decision-making and a smart strategy, small businesses can significantly reduce the threat from cyber attacks.

Challenge

In the last twelve months, **61%** of small and medium sized businesses were victims of a cyber attack[1]. Small business owners face many of the same risks as larger organizations, with fewer resources to devote to cybersecurity.

Policymakers have raised attention to this problem. According to the U.S. National Cybersecurity Strategy:

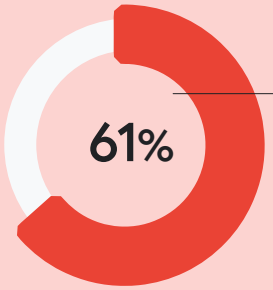
> Today, end users bear too great a burden for mitigating cyber risks. Individuals, small businesses, state and local governments, and infrastructure operators have limited resources and competing priorities, yet these actors' choices can have a significant impact on our national cybersecurity."

Our Solution

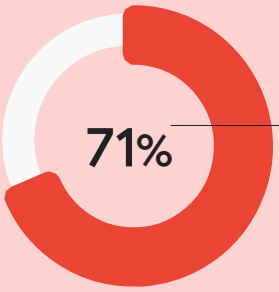
Thankfully, new approaches to security can help ease this burden placed on small businesses. Modern hardware and cloud technologies provide a fast and cost-effective way for smaller organizations to implement the kind of robust security program previously available to only the most well-resourced companies. With cloud, organizations can benefit from economies of scale and robust resources of large providers, who can devote significant resources to keeping software up-to-date.

At Google, we are committed to helping small businesses stay safe online. This document contains guidance to keep your organization secure, and highlights helpful resources.

BlackFog Cybersecurity Research in the US and UK



of SMBs were victims of a cyberattack in the last year



believe they are the selector most at risk for cyberattacks

Four in ten said customer data was lost during the cyberattack

[1] New BlackFog Cybersecurity Research in the US and UK

Google

Security checklist for small businesses

You worked hard to establish your business. Don't let security risks impact your success. Take these security measures to help protect your business information.

If you have a very small business (1-20 users) or small business (21-100 users), you probably don't have a dedicated IT administrator, so we'll keep the list short

Organize for Success

- Make a conscious choice about who "owns" security for your business. If you're a 1-person company, it's you. If you're the founder/CEO, until you specifically task someone else to "own" it, it's still you.
- Choose your technology wisely, and always ensure that security is a key consideration in assessing what products you buy. It's important to understand what risk you're taking on.
- Establish & Encourage the uptake of zero-trust models. Zero trust has been the lynchpin of Google's approach to security since we rearchitected our systems after the Aurora breach in 2010. That's why we launched BeyondCorp Enterprise which brings additional protections against phishing and malware attacks, data leaks and loss - preventing what can be significant harm to the livelihoods of small businesses around the world.

Most organizations would greatly benefit from switching to thin-client devices, Software-as-a-Service collaboration solutions, and managed browsers. Together, these technologies will shift the burden for many security tasks from your organization to the large security teams providing the devices and software. Look no further than how these technologies fare versus ransomware, one of the most pernicious threats to businesses of all sizes. At a time when ransomware is impacting thousands of businesses around the world, there are zero documented cases of ransomware affecting organizations who have adopted a combination of Chromebooks and Workspace.

Protect your accounts

- **Use unique passwords**

  A good password is the first line of defense to protect user and admin accounts. Unique passwords aren't easily guessed. For example, think of a long sentence and use the first letter of each word as your password.

  Also discourage password reuse across different accounts, such as email and online banking.

  Create a strong password & a more secure account

- **Require admins and key users to give extra proof of who they are**

  If someone manages to steal your password, 2-step verification (2SV) can prevent them from accessing your account.

  2SV requires users to verify their identity through something they know (such as a password) plus something they have (such as a physical key or access code) to gain access.

  We recommend that everyone in your business use 2SV, but it's especially important for admins and users who work with sensitive data such as financial records and employee information. You should enforce 2SV for admins and key users.

  Protect your business with 2-Step Verification
  Deploy 2-Step verification

- **Use passkeys to make login easier and more secure**

  Passkeys are a new, passwordless sign-in method that can offer a convenient and secure authentication experience across websites and apps, allowing users to sign in with a fingerprint, face recognition, or other screen-lock mechanism across phones, laptops, or desktop.

  Unlike passwords, passkeys don't need to be remembered or typed and cannot be written down or accidentally given to an adversary. Passkeys are simply easier to use. In fact, Google early data (March – April 2023) has shown that passkeys are 2x faster and 4x less error prone than passwords.

  Administrators can allow users in their organizations to skip passwords at sign-in using a passkey. By default, this setting is off, which means that users can't skip passwords during sign-in, but can still create and use passkeys as a 2-Step Verification (2SV) method. To allow users to skip passwords, administrators can follow these simple steps in the Admin console.

  Allow users to skip passwords at sign-in (beta)

- **Admins should add recovery information to their account**

  If your admin forgets their password, they can click the Need help? link on the sign-in page and Google will send a new password via phone, text, or email. To do that, Google needs a recovery phone number and email address for the account.

  Add recovery options to your administrator account

- **Create an additional super admin account**

  A business should have more than one super administrator account, each managed by a separate person. If your primary super admin account is lost or compromised, the backup super admin can perform critical tasks while the primary account is recovered.

  You create another super admin by assigning the super admin role to another user.

  Assign administrator roles to a user

Google

Get backup codes ahead of time

If your business enforces 2SV and a user or admin loses access to their 2SV method, they won't be able to sign in to their account. Examples are a user who receives 2SV verification codes on their phone and loses their phone, or a user who loses their security key.

In a case like this, they can use a backup code for 2SV. Admins and users with 2SV turned on should generate and print backup codes and keep them in a secure location.

Generate and print backup codes

Keep information on hand for super admin password reset

If a super admin can't reset their password using email or phone recovery options, and another super admin isn't available to reset the password, they can contact Google Support.

To verify identity, Google asks questions about the organization's account. The admin also needs to verify DNS ownership of the domain. You should keep account information and DNS credentials in a secure place in case they're needed.

Security best practices for administrator accounts

Super admins shouldn't remain signed in to their account

Super admins can manage every aspect of your company's account, and can access all business and employee data. Staying signed in to a super admin account when you aren't performing specific administrative tasks can increase exposure to potential malicious activity.

Super admins should sign in as needed to do specific tasks and then sign out. For daily administrative tasks, use an account with limited admin roles.

Pre-built administrator roles
Security best practices for administrator accounts

Enable auto update for apps and Internet browsers

To get the latest security updates, make sure your users enable auto update for their apps and Internet browsers. If they use Chrome, you can configure auto-update for your entire organization.

Auto-update policies (Chrome)

If you use Gmail, Calendar, Drive, Docs

Turn on enhanced pre-delivery message scanning

Phishing is the malicious practice of sending email that attempts to trick users into revealing sensitive information, such as passwords, account numbers, or other personally identifiable information.

Google scans incoming messages to help protect against phishing. When Gmail identifies that an email may be a phishing attempt, it might display a warning or move the email to a spam folder. Enhanced pre-delivery message scanning enables Gmail to help catch email that previously might not be identified as phishing.

Help prevent phishing with pre-delivery message scanning

Turn on additional malicious file and link screening for Gmail

Google scans incoming messages to protect against malicious programs, such as computer viruses. Turn on additional safety checks for attachments, links, and external images to help catch email that previously might not be identified as malicious.

Advanced phishing and malware protection

Make sure email recipients don't mark your email as spam

Email spam is unsolicited bulk email messages. It's generally used by advertisers because there are no operating costs beyond that of managing their mailing lists.

Sender Policy Framework (SPF) is an email security method to authorize legitimate email sent by users at your company. An SPF record identifies which mail servers are allowed to send email on behalf of your domain.

If you don't set up SPF for your domain, some messages could bounce or could be marked as spam.

Authorize email senders with SPF

Restrict calendar sharing with people outside your company

User calendars can contain sensitive information. You should limit how your users share their calendars with external users. Restrict external calendar sharing to free/busy information only.

Set calendar visibility and sharing options

Limit who can see newly created files

You can specify who can see the files your users create. Make sure only the user who creates a file can open it until they explicitly share the file. Do this by turning Link Sharing off.

Set the default for link sharing

Warn users when they share a file with people outside your company

If you let users share files with external people, make sure they get a warning when they attempt to do this. The warning prompts them to confirm that they want to share the file with someone outside of your company.

Don't let users in your organization share with anyone

Google

Does your business have special security requirements?

Your business might have fewer than 10 people but have the information security requirements of a much larger company.

For example, small investment and financial planning businesses, and any business that works with health information might have special regulatory, privacy, and security requirements. These companies might have dedicated IT admins who take care of these extra requirements.

If that sounds like your business, follow the security best practices in the Security checklist for medium and large businesses (100+ users).

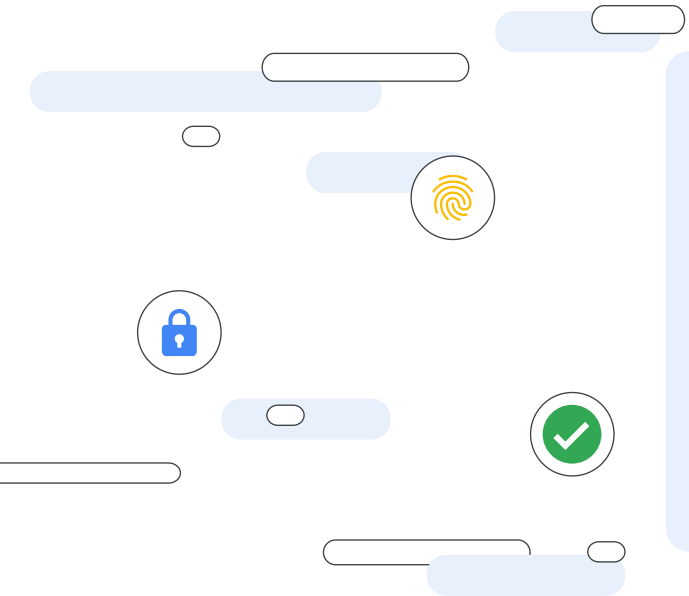
Cybersecurity resources for small businesses

Small Business Cybersecurity Training with Grow with Google

Developed with input from cyber experts at Google, this on demand workshop led by Grow with Google National Digital Coach, Angelina Darrisaw, will introduce the basics of online security and how it applies to your business and customers. You'll learn ways to identify common digital threats and best practices to protect your business, including Google tools you can adopt to increase your business' cybersecurity. You'll also learn about the Google Cybersecurity Career Certificate to help your employees build skills in this space.

Google for Startups Growth Academy

We'll announce the second edition of the **Growth Academy: AI for Cybersecurity**. Growth Academy is an exclusive 3-month program for the most promising startups in Europe and the US, that are using AI technology to grow and innovate responsibly in the Cybersecurity market, with essential growth skills, AI tools, internationalization strategies, and Google products to help them scale. Selected founders will work with a mix of Google experts, such as VirusTotal and Mandiant, AI engineers and external industry leaders in a series of workshops and will receive mentoring across strategy, sales, and partnerships. The application window is open from Oct 2nd to Nov, 12th.



At Google, we are more focused than ever on **protecting** people, organizations, and governments by sharing our expertise, **empowering** society to address ever-evolving cyber risks, and continuously working to **advance** the state of the art in cybersecurity to build a **safer world for everyone**