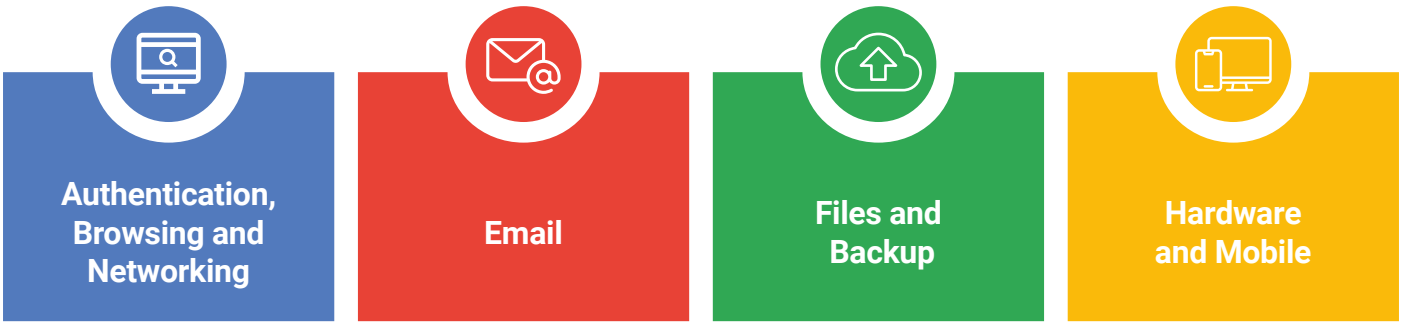
On Opennetworks

Security Coverage Checklist

What you need to know to secure your data and communication.

Security is about technical matters and technology. When Opennetworks talks about security we mean all the technology and technical considerations that are relevant for the current and future of cloud computing. That is, everything from passwords, to encryption, to hardware, to administrative configuration and more!

There are 4 Areas that you need to consider when looking at your security coverage.
These are:



In this document we are going to cover some of the steps that you need to take in each of these areas to secure your data and communication.

Authentication
This is about how you log into your services, proving that you are authorised to access them.

Browsing
This is about safe web browser usage and safe applications access.

Networking
This is about the things that happen in the background to connect you to the services you use.

On Opennetworks

Security Coverage Checklist

- [ ] **Passwords should be at least 8 characters long and should be easy for you to remember.** (Pro Tip: It's better to have a password like "VolkanoOrJBLWhichIsBetter?" than "1h7yuER!z")

- [ ] **Set up Two-Step Verification on all accounts.** (Pro Tip: For extra security, add Two Factor Authentication to the process as well.)

- [ ] **Share super administrative access between key individuals within the organisation to ensure that you can regain access to your data and accounts if an account has been compromised.** (Pro Tip: There should be someone whose role it is to monitor activities by those with system access.)

- [ ] **Ensure that employees are using native apps. Applications have certain security features that are standard and specific to the application. By using 3rd party apps to access information (such as Outlook to access your Gmail) you are compromising your data security.** (Pro Tip: Set up a policy and procedures document that covers which 3rd party apps/extensions you want your users to have access to - if at all.)

- [ ] **Configure policies for browsing, mobile device usage, and app usage for your organisation. This allows you to determine which applications your organisation can access, which networks they use and so much more.**

- [ ] **Ensure that your list of domains that are blacklisted is up to date and the necessary steps have been taken to block all emails received from these domains.** (Pro Tip: To keep company information safe, with Google Workspace you can also set up notifications to alert employees of emails being sent to external domains.)

- [ ] **To track and keep the distribution of documents and data in check, store all documents in one central location. This should ideally be with a cloud solution.** (Pro Tip: With Google Drive you can regulate access to your files on account, group and organisational levels.)

- [ ] **Enable software encryption in the creation and (especially) the sharing and storing of your data.** (Pro Tip: Google's services are encrypted by default.)

- [ ] **Set up mobile device management. Decide on the manner in which mobile devices (i.e. phones and tablets) that access your domain and data are used. For example, making it mandatory that phones that access company accounts have a screen-lock.**

- [ ] **Understand the signs of phishing and virus emails. Set up a checklist of what to look out for when opening and reading emails that will empower employees to spot dangerous and malicious emails.** (Pro Tip: Google Workspace offers businesses the option of setting up notifications to automatically warn the email recipient of possible dangerous emails.)

On
Opennetworks

But wait...

there's more!

These are 10 of the basic steps that you can implement as a business owner to start protecting your data and communication. The 4 Areas that you need to consider when looking at your security coverage include more in depth steps and processes that, when implemented correctly, give you the peace of mind knowing that your business can function efficiently and securely.

When it comes to ensuring the security of your data and communication, look no further than Google Workspace. Stay connected, work and collaborate together, and do all of this securely. Making the shift to cloud computing means that you can increase your productivity, better team collaboration, increase your data security, and reduce IT costs.

So, how does Opennetworks help our Google Workspace customers?

1. 2 Step Verification with Change Management

We not only help you set it up but plan how you do so with advice for how your teams should best use it.

2. 10 Point Security Analysis

We conduct a best practice wide surface review of your Workspace security to:

- (i) Reduce the technical surface area vulnerable to security compromise and,
- (ii) Enforce awareness of risky account usage.

This covers everything from email setup, to 3rd party applications and employee-related processes (including on-boarding and off-boarding procedures).

3. Security Incident Response

Our specialist team conducts an emergency response to eliminate any threats and limit the impact. We establish a boundary in time that contains the incident and provide you with a report for legal and governance purposes.

4. Custom Security Audit

This product is a targeted audit and configuration of a specific security surface area.

5. Custom Security Workshop for Technical Teams

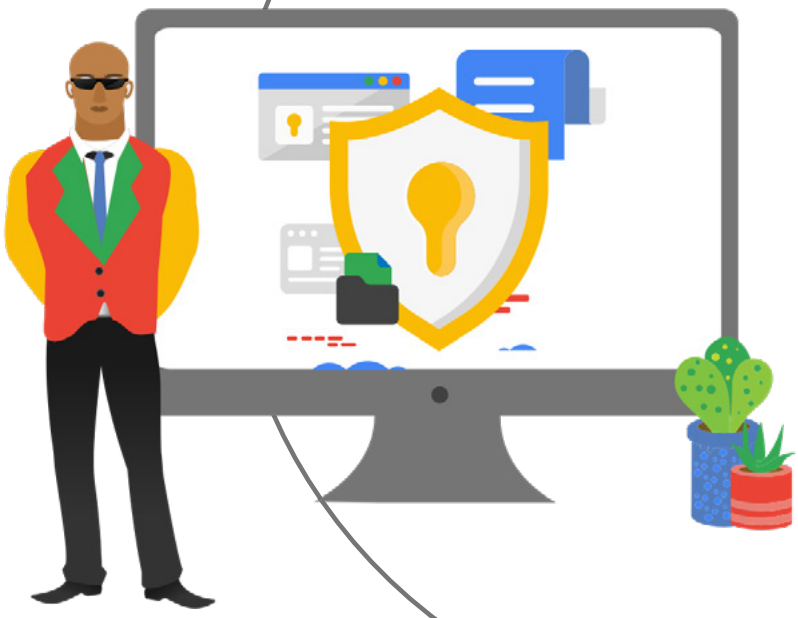
We empower your techies to manage your Workspace security with an in depth workshop that also covers the tips we have learnt over the years.

To find out how Opennetworks helps your business take advantage of he collaboration Workspace that drives real change in your organisation, go to:

opennetworks.com

On Opennetworks

On
Opennetworks



Contact Us

Sales@opennetworks.com
+27 (011) 073 3860

Google Cloud Partner

Google for Education Partner

monday.com Gold Partner