Small Business Guide to Cloud Services

Andrew A, James L1; Platform Security Research

Many businesses rely on cloud services every day – whether it be for e-mail, storing documents, tracking your accounts or engaging with your customers over social media. In doing so, we're getting someone else to take responsibility to keep those services running every day, and make sure they're built and managed with security in mind.

The advice below builds on our Small Business Guide to Cyber Security, to help you use those services in a way that will make it less likely that your business will be a victim of cyber crime.

We have focused on the features that are available in services such as Google G Suite and Microsoft Office 365. Many of the tips will also apply to any other online/cloud services that your business relies on.

Securing your users' accounts

Cloud services are usually designed so that you can log on to them from anywhere on the Internet. There are a few things that you can do to make it difficult for someone else on the Internet to gain unauthorised access to your accounts.

You can find more information about protecting your data with passwords – including when it's on your devices – in the Small Business Guide – Step 4.

Tip 1: Avoid using guessable passwords

Passwords should be easy to remember, but hard for somebody else to guess. A good rule is 'make sure that somebody who knows you well, couldn't guess your password in 20 attempts'. You should also avoid using the most common passwords, which criminals can easily guess. The NCSC has some useful advice on how to choose a non-predictable password.

Tip 2: Use unique passwords for each account

Attackers use a variety of techniques to discover passwords, exploiting a range of social and technical vulnerabilities, as explained in our password policy guidance.

We recommend that you use a unique password for each online account and service that your business relies on. This means that if one of your passwords is stolen, it will only give access to a single service used by your business, and not all of your e-mail, social media and bank accounts in one go.

To help you deal with more than one password, you may wish to write them down and keep them locked away somewhere safe. You may also consider using a digital password manager, which is a tool on your device that can create and store passwords, and protected using a 'master password' or biometric.

Tip 3: Use two-factor authentication

Make sure that you take the option to use two-factor authentication (also known as 2FA) for all of the accounts that give access to services that your business relies on; it adds a large amount of security for not much extra effort. It's also a good idea for any other online services you use, if they offer it.

2FA requires two different methods to 'prove' your identity before you can use a service, generally a password plus one other method. This could be pressing an approve button in an app or a code that's sent to you that you must enter in addition to your password.

The NCSC has separate guidance about 2FA that explains some of the options and how to use them.

Using 2FA can stop some older applications from working if they rely on less secure methods to access your data. You should be able to continue using an older application by creating an 'App Password' for your account. This allows you to use a traditional username and password for that application while benefiting from 2FA security everywhere else.

Protecting your most powerful accounts

Some services are designed so you can issue standard accounts to several people, using a more powerful "administrator" account. One or two people are usually responsible for paying for the service, and setting up/managing the accounts of others.

Attackers can do more damage if they can get access to these administrator accounts, as they have access to information held by all of your staff. Additionally, having access to one can help you recover if one of your users is breached. There are a couple of extra things you can do to these accounts.

Tip 4: Limit the use of administrative accounts

An attacker can access more data and do more damage if they successfully break into an administrator account. You should therefore only give one of these accounts to the people in your company that are responsible for the IT.

It's a good idea to have more than one administrator account, each managed by a separate person. This means that if one of those accounts is lost or compromised, a second one can be used to start cleaning things up, while the first is being recovered.

You should log out of administrative accounts when you're not specifically performing administrative tasks.

Tip 5: Add recovery information to administrative accounts

If you lose access to an administrative account, you will need to get the service provider to help you to get back in. You should make sure that any e-mail addresses, phone numbers and postal addresses are kept up to date so that you can be sent new credentials.

If you're asked to set a backup e-mail address, you should make sure it's entirely separate from your main one – run by a different provider and using a different password.

Some providers may also ask for information about your organisation when you call them to verify that you're you – so you should make sure that the information provided to them is correct.

Tip 6: Protect the account used to manage your custom domain name

Many organisations use a custom domain name – such as ncsc.gov.uk or getsafeonline.org – for their e-mail addresses and website. In fact, some cloud services require it. If you have a domain name, you should follow Tips 1-4 above to protect the account used to manage it.

Defending your online accounts from malware

We normally think about viruses or malware as something that infects and damages our physical devices. However, some malware is also designed to steal passwords to online services. You can reduce the risk of this happening by only using your business's cloud services from devices that you have a reason to trust.

Tip 7: Keep your devices healthy

You should make sure that the devices that you're using to log in to your cloud services are healthy and up to date.

For all your IT equipment (including tablets, smartphones, laptops and PCs), you should make sure that the software and firmware is always kept up to date with the latest versions from software developers, hardware suppliers and vendors. This applies to the device itself, as well as the web browser and any apps you've got installed. Applying these updates (a process known as patching) is one of the most important things you can do to improve security, and can often be set up to be done automatically.

Antivirus software - which is often included for free within popular operating systems - should be used on all computers and laptops. For your office equipment, you can pretty much click 'enable', and you're instantly safer. Smartphones and tablets might require a different approach and if configured in accordance with the NCSC's EUD guidance, separate antivirus software might not be necessary.

You can find more information about protecting your organisation from malware in the Small Business Guide – Step 2.

Tip 8: Only use devices that you trust to access your online services

You can usually get some confidence that the devices that belong to your business, and often the personal ones belonging to your staff have some defences against malware. However, you should never log on to your business accounts from a device that you don't have reason to trust – such as one in a hotel or internet café.

Use the security features built into the service

Many cloud services have security features built in to help defend you and your data against cyber attack. Sometimes these are turned on by default, but sometimes you have to turn them on yourself. You should therefore check that you're using them.

Tip 9: Filter out malicious email and files

Many cloud services include filters that help protect you from phishing, spam and malware. You should check that these are all turned on, including any optional features that are included in your subscription.

These features will help you avoid phishing attacks, which you can read about in the Small Business Guide – Step 5.

Tip 10: Prefer the apps provided by the cloud service

Many cloud services are designed to be accessed via a web browser or via an app provided by the service. We recommend using these methods, rather than a more generic e-mail app or 3rd party

app. The web interface and supplied apps are often designed to help you make good security decisions for that specific service

You should avoid third-party apps if they require you to adjust or weaken the security configuration of the cloud service in order to make them work.

Tip 11: Back up the data that's critical to your business

Even if you use the cloud, you still need to consider how you go about backing up your data, and restoring access to it if the worst happens. You should refer to the Small Business Guide – Step 1 to come up with an approach.

Some cloud services keep older versions of your files. This means that if you are subject to a ransomware attack, you may still have a recoverable copy of the files as they were prior to the attack. Some cloud services also keep a copy of your deleted files for a short period – the provider may be able to recover files that an attacker deleted from your cloud service.

You should however not rely on these mechanisms for your most important data, and instead ensure that you keep an independent copy as described in a recent blog.

Implementing this guidance

While the same tips usually apply whichever cloud service you're using, the way you actually implement them will vary. You can usually find configuration guides on a service's website. Some useful references we've found are:

- G Suite: Security checklist for small businesses (1-100 users)
- Office 365: Top 10 ways to secure Office 365 and Microsoft 365 Business plans

Recovering a hacked account or service

You may discover that someone else has gained control of your account by some obvious sign, such as you can't get into it one day. Sometimes the signs are more subtle – such as changes to security settings, password reset attempts, or messages being sent from your account that you don't recognise.

You should familiarise yourself with our guidance about recovering a hacked account which explains some steps we recommend you take if you find yourself in this situation.

Each cloud service will have a different process to recover your account, either by yourself or with their help. You may find these step-by-step guides are useful:

- G Suite: Reset a user's password, Reset your administrator password, reset access from all devices and Identify and secure compromised accounts
- Office 365: Reset Office 365 business passwords , reset existing access and How to fix a compromised (hacked) Microsoft Office 365 account