7 cybersecurity practices for small businesses

Our easy guide on how to start protecting your business.

Cyber Accelerator Alumni

in association with National Cyber Security Centre

CYBER ESSENTIALS

naq.

1

Get creative with your passwords:

Use unique, strong passwords for every single one of your accounts.

Using strong and unique passwords for each account is one of the most effective things can do to reduce the chances of your accounts being compromised.

Even if your password is strong, if you're using the same one across all of your online accounts, a single data breach can suddenly put the remainder of your data at risk.

Begin by installing a password manager such as **LastPass** which can automatically store and fill out your log-in information. You can easily ensure every single one of your accounts has a unique password, without needing to remember them or note them down.

Password guessing is an incredibly common method used by cybercriminals in order to get access to accounts. If any of your passwords follow the common "company123" pattern, change these immediately.

2

Turn on two-factor authentication:

An additional layer of security for your accounts.

Two-factor or multi-factor authentication offers additional layers of security beyond a straightforward password.

With two factor authentication (2FA), **even if someone gets hold of your password, it is unlikely they will be able to access the additional information required to complete the second step of the verification process.**

2FA usually allows you to verify via email, through the use of an autheticator app or a receive a unique code to your mobile, meaning you and only you have access to your account.

3

Secure your connections:

Ensure your company networks are secure, wherever you work from.

Wherever you are, in order to work, you'll need to connect to a network. Whether it's your home or office network, it is crucial that your network is configured securely.

Begin by changing your WiFi name and that standard password provided by your internet provider if you haven't done so already.

Even if you've configured your WiFi securely, you should always use a **Virtual Private Network** or VPN to secure the connection between your computer and the internet. NordVPN is a great, affordable VPN provider.

4

Beware how you share

Limit your amount of shared information & secure your shared drives.

In small businesses, there is always the need to share information. Sharing personal data is personal reasonable and GDPR compliant as long as you take adequate measures to protect that information.

Always check whether the people with whom you're sharing data really need access to that information If the answer is yes, share this information via a secure cloud platform as opposed to an email attachment. **Cloud services include Google Drive, Dropbox or OwnCloud.**

Once your recipient has finished using the information, remember to disable any shared links in order to keep your data secure.

5

Don't bring your own device:

Limit your use of personal devices for work

Working from home, or a sunny island means freedom to use personal devices to do your job. but that increases the risk to your business and the sensitive information it is responsible for.

Make sure you only use your work devices. These should have an antivirus and firewall installed. Additionally, these could be backed up or wiped remotely if necessary. And remember to only use your work device for, well, work.

6

Take a break, get coffee and update.

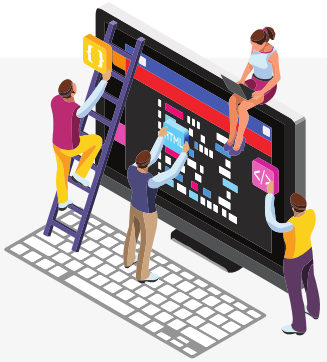
Ensure your devices are updated automatically.

The well-known pop-up that says "there's a new update available" isn't just annoying (we admit it), but an extremely important part to securing your device and your business' information.

When we ignore those pop-ups, or simply keep postponing, we are giving criminals the perfect opportunity to exploit the little holes in our software or operating systems that updates are intended to repair.

7

Backing up can be a lifesaver



Get access to your data, even if the worst happens.

Imagine, it's later and you've almost finished your work for a client. You've stepped away from your desk, and when you return, you notice the worst has happened. Your laptop has crashed.

In instances like these, wouldn't it be great if you had a backup? Make sure to always back up your data to a cloud service provider. Ideally, back up your data to a cloud backup provider such as **CloudAlly.**

naq.

About Naq

Naq provides SMEs with a complete cyber security, GDPR compliance and staff training solution at an affordable monthly cost. Through our exclusive easy to use platform businesses can review their security actions, improve their organisation's security score and ensure their staff are trained on the most common cyber threats. **All delivered for as little as €99 a month.**

GDPR & DPA Compliance

We provide businesses with complete and bespoke data compliance policies ensuring their data and marketing efforts remain compliant.

Cyber security & Monitoring

24/7 monitoring, web scanning & easy to implement actions to protect your business' valuable data.

Staff Training & Phishing Tests

Training courses & phishing tests to empower your team to remain compliant & secure

Incident Response

if your business falls victim to an attack, we'll be there to help with data recovery and legal advice.

Ready to begin protecting your business?

Take a look at our pricing page here. Alternatively, reach out to us on info@naqcyber.com and a member of our team will be in touch.

Cyber Accelerator Alumni

in association with National Cyber Security Centre

CYBER ESSENTIALS

naq.