SECURITY

IT - Security

Managed Anti-Virus
Any business of any size requires managed anti-virus to help protect against malware, trojans and spyware, this should be mandatory. Our managed anti-virus will provide a level of protection against many threats, and even if it unable to successfully neutralise a threat, it will send alerts where manual intervention is required. With approximately 200,000 new malware strains detected every day on average, it's important to keep the anti-virus up-to-date. Our managed anti-virus will alert us if a computer hasn't received its patches, so we are able to take corrective action. We can remotely push any updates to computers, configure deep scans to run immediately and manage any potential false negatives, all without having to disturb the user from their work.

Web Filter
Most of the cyber threats today are generated from the web. It goes hand in hand with our reliant on web based applications and requirements. Sophisticated threats such as Social Engineering and Trojans can often trick staff into thinking they are on a genuine website. Having a web filter will not only assists in blocking access to dangerous websites, but can also increase productivity by preventing staff from accessing social media, gambling or shopping web sites.

E-mail Filter
E-mail is the life line to most business communications, and hackers know this. It's why E-mail is such a popular vehicle for hackers to initiate their attacks. Most people have heard about phishing attacks but are not aware what to look for, and with Spear Phishing (a more targeted attack on a certain business) becoming more frequent, it's starting to get extremely difficult to differentiate between genuine e-mails and potential threat e-mails. Which is why having a SPAM filter will heavily reduce risk of a user unintentionally allowing threats to attack your IT Systems.

Our SPAM filter sits in the cloud and act as a gateway to your e-mail server. It will be the first point of entry and the last point of exit for all business emails. This enables us to stop most of the threatening e-mails before they even hit your network. It will also enable us to identify any potential viruses on internal devices sending out unauthorised emails. In addition it will save resources on your internet line and email server, not having to deal with processing large numbers of unwanted data, as well as saving user's time not having to delete or mark unwanted email as junk. The users will get a daily email showing all threats which have been quarantined, and give them the option to release any false positives, ensuring you won't miss any important emails.

VDI

One of the most common ways of losing data is having computers lost or stolen. With GDPR regulations, if a computer is lost or stolen and it holds sensitive data, it will need to be reported within 72 Hours. By implementing VDI, none of the data will leave the servers it is located on. Any loss of physical devices will not hold any sensitive data, essentially they are just used as a terminal to access your workspace. This means more control over who as access to company data and from where, it also means a single environment to focus your security on.

Wi-Fi Security

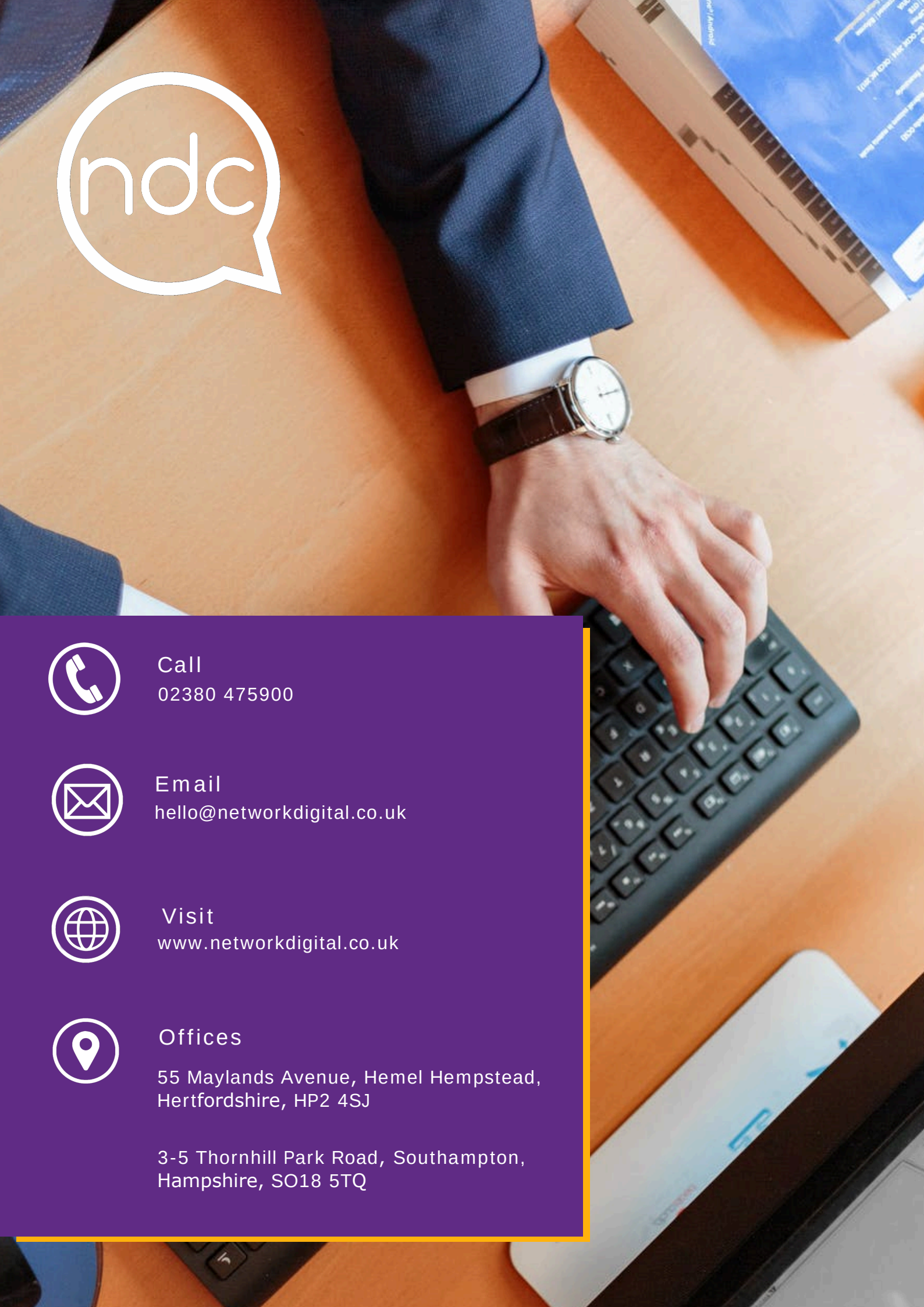
All businesses will have Wi-Fi in some shape or form. Most of which will be setup from the internet providers and used straight out of the box. Wi-Fi can pose a big security threat if not setup correctly, it's one of the easiest way to penetrate a network. Make sure you're not accidentally leaving your network exposed making it easy for hackers to target and compromise your networks. Once a hacker gains access they can attack your computers, servers, mobile devices (usually) undetected in order to obtain usernames, passwords or data. Which can all be held to ransom.

Firewall

A secure firewall is another essential in protecting your IT systems. The point of entry from the public internet to your private network, your firewall is essentially the front door to your house. Front doors come in all shapes and sizes, as do firewalls. No doubt the internet router/modem from your internet provider has a built-in firewall, but they are generally a basic form of firewall offering you a basic form of protection. You should be running a firewall which has active updates, giving you protection against the latest published threats. A firewall that has granular settings so that you are able to safely run business essential services, without making it easy for hackers to penetrate. You wouldn't have a poor lock on the front door to your house, so make sure you don't have a poor firewall on the front door to your network.

Two Factor Authentication

Passwords are a big part of our lives now, and with so many to remember staff tend not to put as much complexity with their work passwords as they would do their personal banking passwords. Yes you should have a password policy in place which forces a complicated passwords, but even with this, staff tend to use the same or similar variants of their work passwords. They openly share these with colleagues or write them down on a post-it note on their monitors. Two Factor Authentication removes the risk from the user by introducing a secondary authentication method, be in a text message with a code, or a fob with a random set of changing numbers. This method of logging into systems is much more common place now and people welcome the extra layer of security which keeps their money safe or protects their credit card transactions. Protecting your business data should be equally as important to you.



Call
02380 475900

Email
hello@networkdigital.co.uk

Visit
www.networkdigital.co.uk

Offices

55 Maylands Avenue, Hemel Hempstead,
Hertfordshire, HP2 4SJ

3-5 Thornhill Park Road, Southampton,
Hampshire, SO18 5TQ