DEMYSTIFYING DNS

Why DNS is essential to your cyber security

NOMINET
CYBER
SECURITY

Introduction

As the cyber security landscape evolves, and sophisticated online criminals prey on large organisations that don't have the right defences in place for a modern-day onslaught, cyber security is now ranked as one of the major challenges facing CEOs today.

Gartner research shows that IT-related changes are the number two business priority for CEOs, ranking second only to growth. This is due to a shift away from outsourcing with 57% of CEOs preferring to build up digital capabilities in house, the reinternalisation of IT. And with the General Data Protection Regulation (GDPR) in place since May 2018, businesses need to ensure they have a robust security solution – policy, resources and tools in place or they could be at risk of significant fines.

91% of CEOs say breaches of data privacy and ethics will have a negative impact on stakeholder trust in the next five years.

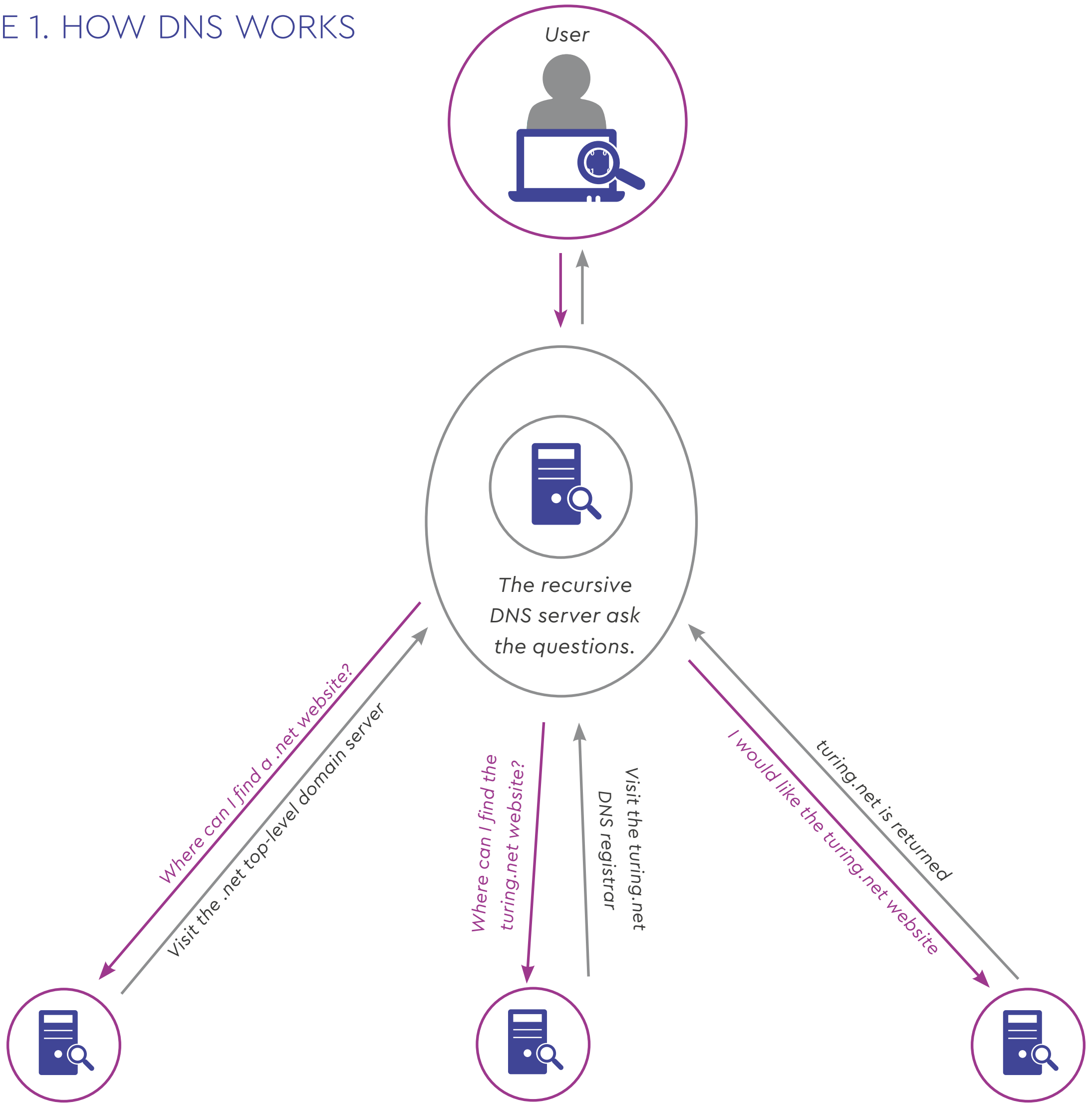
Source: 20th CEO Survey, PwC, 2017

The role of DNS

DNS plays a critical role in every network – it is the technology standard used to turn humanly understandable domain names into internet protocol (IP) addresses understood by machines.

For example, when someone types in the website **www.example.com**, this is converted into IP address **93.184.216.34** and a data lookup takes place to ensure the right site is returned. This makes it quick and simple to access websites, applications and devices on the internet, do business online, socialise, learn and collaborate.

FIGURE 1. HOW DNS WORKS


User
The recursive DNS server ask the questions.
Where can I find a .net website?
Visit the .net top-level domain server
Where can I find the turing.net website?
Visit the turing.net DNS registrar
I would like the turing.net website
turing.net is returned

AUTHORITATIVE ROOT SERVER

The root server handles requests for information about top-level domains only and does not have the information about where the lower-level domains (or full domain name e.g. turing.net) are hosted. The job of the root server is to direct the requester to the name servers that specifically handle the requested top-level domain.

AUTHORITATIVE TOP-LEVEL DOMAIN SERVER

These servers give answers to queries about the domains under their control (e.g. .com, .net, .uk). There are multiple top-level domain servers so your query for .com will be directed to a different location than your query for .uk. The top-level domain servers are authoritative as they provide the address of the requested domain's DNS registrar or private DNS server.

AUTHORITATIVE DOMAIN-LEVEL NAME SERVERS

These servers contain the details for the requested domain, usually known as zone files. The zone file holds both the domain name (e.g. nominet.com/cybersecurity and the machine readable IP address for that host. This returns the final answer – the IP address – to the requester and is the last stage of the domain name system.

The role of DNS

DNS is easily accessible to everyone – users with good intentions and, unfortunately, the criminally-minded alike. Several factors make DNS especially attractive to cyber criminals. Due to its ubiquitous, always-on but behind-the-scenes nature, DNS is often overlooked by system administrators. It has some inherent vulnerabilities coming from its design, to be an open and easy-to-operate system. Most firewalls whitelist DNS. This results in DNS becoming a path for many cyber attacks.

For example, cyber criminals can easily manipulate a targeted company's domain name for malicious purposes. They can also easily register domains that differ only slightly from an organisation's legitimate domain name (known as 'typosquatting') or redirect traffic that's navigating to the company's website to a rogue server by altering the IP address mapped to that domain in DNS records. Criminals use these techniques routinely to carry out scams, such as phishing, click fraud or brandjacking.

The number of attacks exploiting DNS are on the rise. Organisations worldwide are facing an immediate need to pay closer attention to DNS, to detect and respond to attacks, in order to keep their business secure and protected. Fortunately, due to the pervasiveness of DNS it's a great place for plugging in a defence layer that offers protection from threats that traditional security solutions, such as antivirus or network firewalls, would miss.

With the growth of the internet and more and more people and devices getting online every hour of every day, there are billions of packets of data to monitor, track and analyse. Traditionally it has been very difficult to gain insight into DNS traffic and to detect cyber threats or identify network misconfigurations that affect performance. There is now a business need to tap into this wealth of data and make sense of it.

DNS on your corporate network

Corporate recursive DNS server

If your organisation has a significant online presence, you're probably running your own DNS server. For example, a recursive DNS resolver which intercepts all outgoing queries to the internet from your organisation's users, such as a user clicking on a link to connect to to a website.

Then, to find the IP address of the server that hosts the requested website, the recursive DNS resolver either forwards the query on to other servers or, if it has received the answer previously and cached it, it replies to the user right away.

These servers can be targeted by cyber criminals in several ways:

- Altering the answers to the queries that the server stores can redirect users to a malicious website and lead to a malware infection or loss of confidential data, for example, through phishing (see figures 2 and 3)
- Unauthorised copying and transfer of confidential data can be leaked through DNS, this is known as data exfiltration (see figure 4)
- Denial of Service (DoS) attacks can overload the DNS servers and shut down DNS resolution for a network, so that queries coming from real users trying to connect would not resolve and the website would not be displayed, thus disrupting business (see figure 5)

By analysing traffic that goes through the recursive servers, Nominet's security solutions can tell you a lot about the health of your network. For example, by monitoring traffic while cross-referencing the security lists it can reveal infected machines on your network, such as machines that have become part of a botnet and are sending spam, or those contacting a command-and-control domain after they've been infected with malware that uses that domain to establish a communication channel.

FIGURE 2. PHISHING

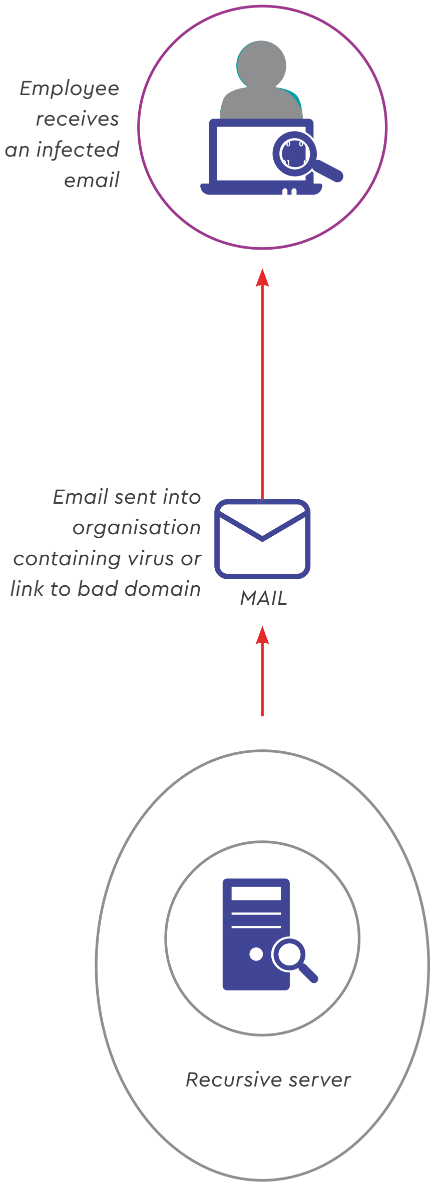

Employee receives an infected email
Email sent into organisation containing virus or link to bad domain
MAIL
Recursive server

FIGURE 3. MALWARE

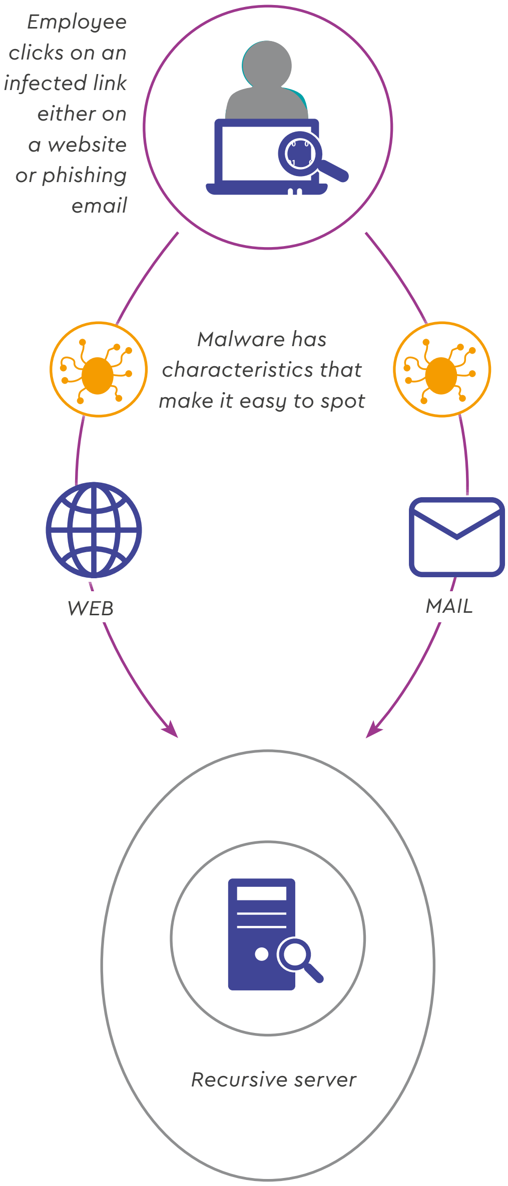
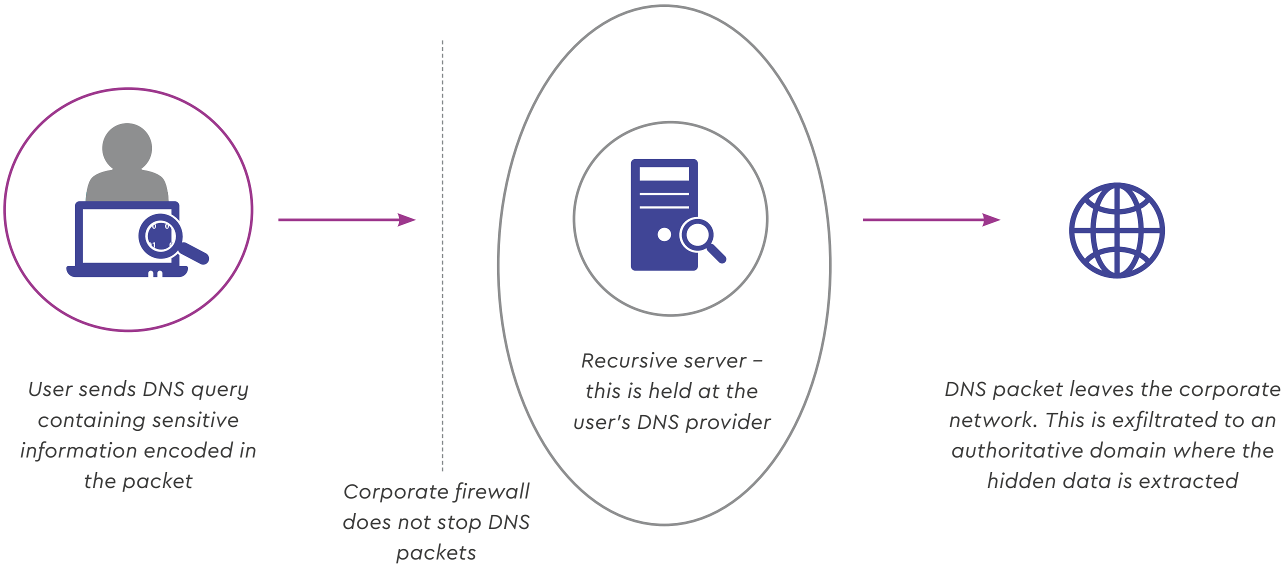
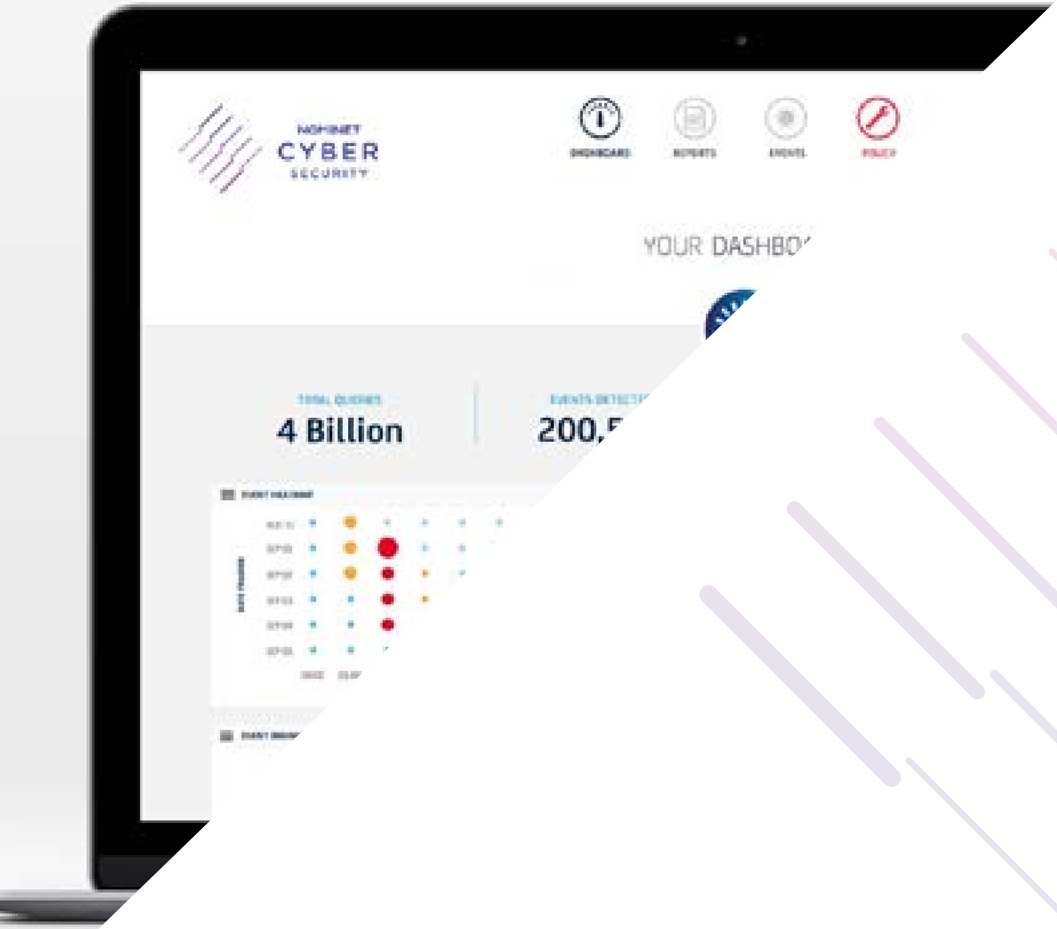

Employee clicks on an infected link either on a website or phishing email
Malware has characteristics that make it easy to spot
WEB
MAIL
Recursive server

FIGURE 4. DATA EXFILTRATION


User sends DNS query containing sensitive information encoded in the packet
Corporate firewall does not stop DNS packets
Recursive server – this is held at the user's DNS provider
DNS packet leaves the corporate network. This is exfiltrated to an authoritative domain where the hidden data is extracted



Corporate authoritative DNS server

As an organisation you have an external audience, they will be asking your website questions:

Where can I find the latest product?

What are the details of your service offering?

How much does it cost?

Providing them with the right answers is authoritative DNS.

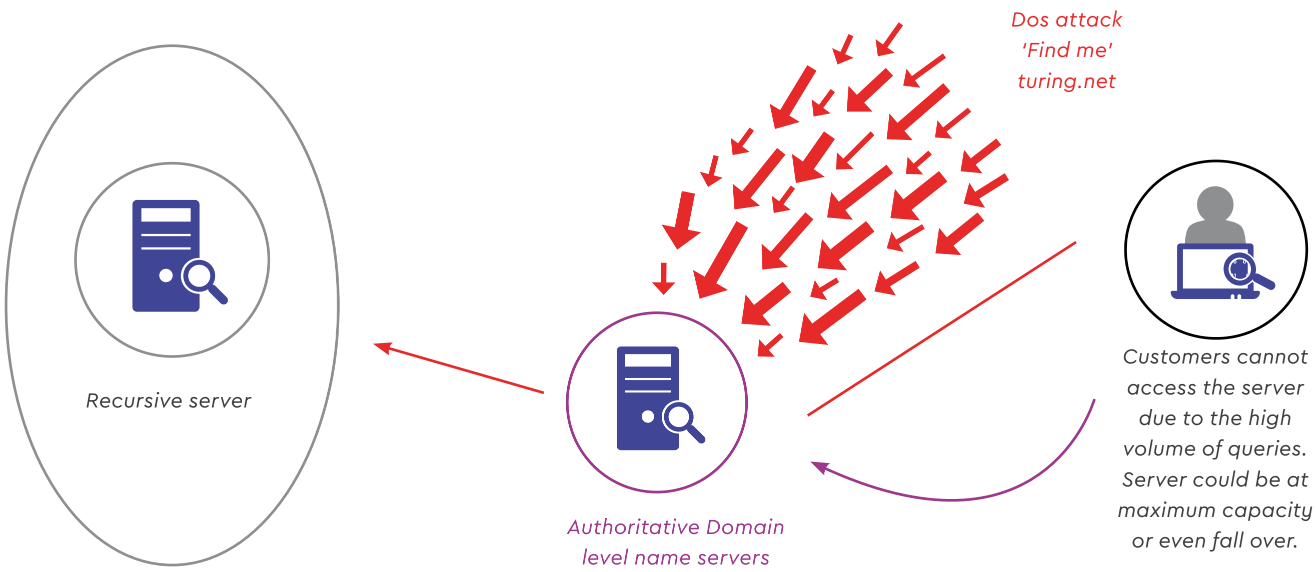
You will be running an authoritative nameserver, this server is responsible for answering these questions, mapping your domain names to IP addresses of the servers that host them and returning the right results to your customers. Tampering with the records the nameserver holds or its load and availability can seriously harm your business. Protecting this asset is of paramount importance to the operation, security and reputation of your business.

A DoS attack against an authoritative DNS server may shut down resolution for a specific domain name or a group of domain names, so that no users can access them. An example of such an attack and the impact it may have is a DDoS attack, a type of DoS on Dyn which took place in November 2016[1] (see figure 5).

During a DNS hijack, cyber criminals redirect traffic intended for a company's website to their web server with a replica of the site's content. Once on the fake site, users could enter user accounts, passwords, or even credit card numbers. In April 2017 hackers redirected all traffic intended for a Brazilian bank to a phishing replica of the website, and stole users' bank account details.[2]

Nominet's security solutions come with built in DNS analytics capabilities that can detect suspicious traffic, as well as unfolding DoS attacks right from the start. It also provides you with all the details of a security event that enable you to act promptly and mitigate the threat - for example, IP addresses responsible for a DoS attack that you'd want to block, stopping your servers from falling over.

FIGURE 5. DOS



[1] (https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/)
[2] (https://www.wired.com/2017/04/hackers-hijacked-banks-entire-online-operation/)

ISP recursive DNS server
Delivering DNS Services to your customers

If you are an Internet Service Provider running a recursive DNS name server for your customers, making and caching queries on their behalf, then adding a security and analytics layer to this service can enhance your proposition, helping to protect your customers and your own organisation.

In addition to identifying threats and other events discussed in the previous sections of this paper, Nominet's security solutions can also provide invaluable insight into your customers' business and browsing habits. For example, the list of top domain names can help you to better understand what people are most often looking for. If you are hosting websites, identifying the most popular hosted websites can help you allocate your resources so that those sites always have enough bandwidth. You can spot the latest fad website or see this information at different times or days of the week, to help you identify patterns and manage resources allocated to hosted sites to improve load balancing (see figure 6).

The top source IP addresses can help you to better understand who your users are. By identifying where your traffic is coming from, you can, for example, reduce your internal costs by setting up appropriate peering arrangements that would allow you to manage the traffic in the most cost-efficient way to you.

Nominet's NTX platform can give you insight into this customer behaviour as well as helping you identify and mitigate against security risks.

What is Nominet's security solution?

The Nominet Cyber Security Services enable your security team with unique insight into cyber threats inside your organisation and the capability to find and fix problems that no other service can touch. Our responsive, reliable, scalable and secure DNS service protects your business by detecting cyber threats in realtime and blocking access to reported malicious sites and malware variants in flight.

Based on over 20 years of national-scale DNS expertise and eight years of dedicated research, we have a unique insight into cyber threats, and the capability to find and fix problems that no other service can touch. Our unique, patented compression and analysis algorithms, derived from the fields of acoustics and holography, allows you to capture, understand and visualise the threats contained in your DNS traffic.

Flexible Security Services

Protect your users the way it suits your business:

Nominet NTXprotect – our standalone technology, installed on-premise or cloud-delivered, for use by your in-house security team.

Nominet NTXsecure – our fully managed DNS service overseen by a team of experts.

About Nominet

As the registry for the .UK domain, Nominet have two decades of experience in network analytics and protection. We built our worldwide patented DNS analytics tool to help us understand and protect activity on the UK internet – so we know it works. Nominet are part of the Active Cyber Defence Programme run by the National Cyber Security Centre in the UK, providing the UK Public Sector DNS service to the UK government departments.

Nominet is driven by a commitment to use technology to improve connectivity, security and inclusivity online. A profit with a purpose company, Nominet supports initiatives that contribute to a vibrant digital future.

NOMINET
CYBER
SECURITY

For more information on how Nominet can help secure your business, please contact us
www.nominet.uk/cybersecurity