Security White Paper

Router Operation Best Practice

Abstract:

If you own, install or operate a broadband router or any kind of wireless LAN, you and your users are a target. This white paper summarises the most important practices that you need to adopt to reduce your chances of becoming a victim and seeing your company or private data being compromised, regardless of your chosen equipment vendor.

DrayTek


DrayTek

Introduction

Corporate espionage, stealing financial data or hacking governments are the most interesting or most rewarding exploits for a hacker but every network is a potential victim. You might not have valuable corporate data to steal, but you do have banking transactions, private documents or computers which could be hijacked for botnets. Every vulnerable network or computer is of interest to a hacker, and if your home network is connected to your work network, or work email, exposing your home network exposes your employer's network too.

Even with the best locks and the strongest doors, if you or a member of your staff fail to operate them correctly or don't apply recommended precautions, those locks might be no better than poor quality or no locks. This same principle applies to your computer network; all of your network components and in particular your router, which is the gateway between your network, your users and the Internet.

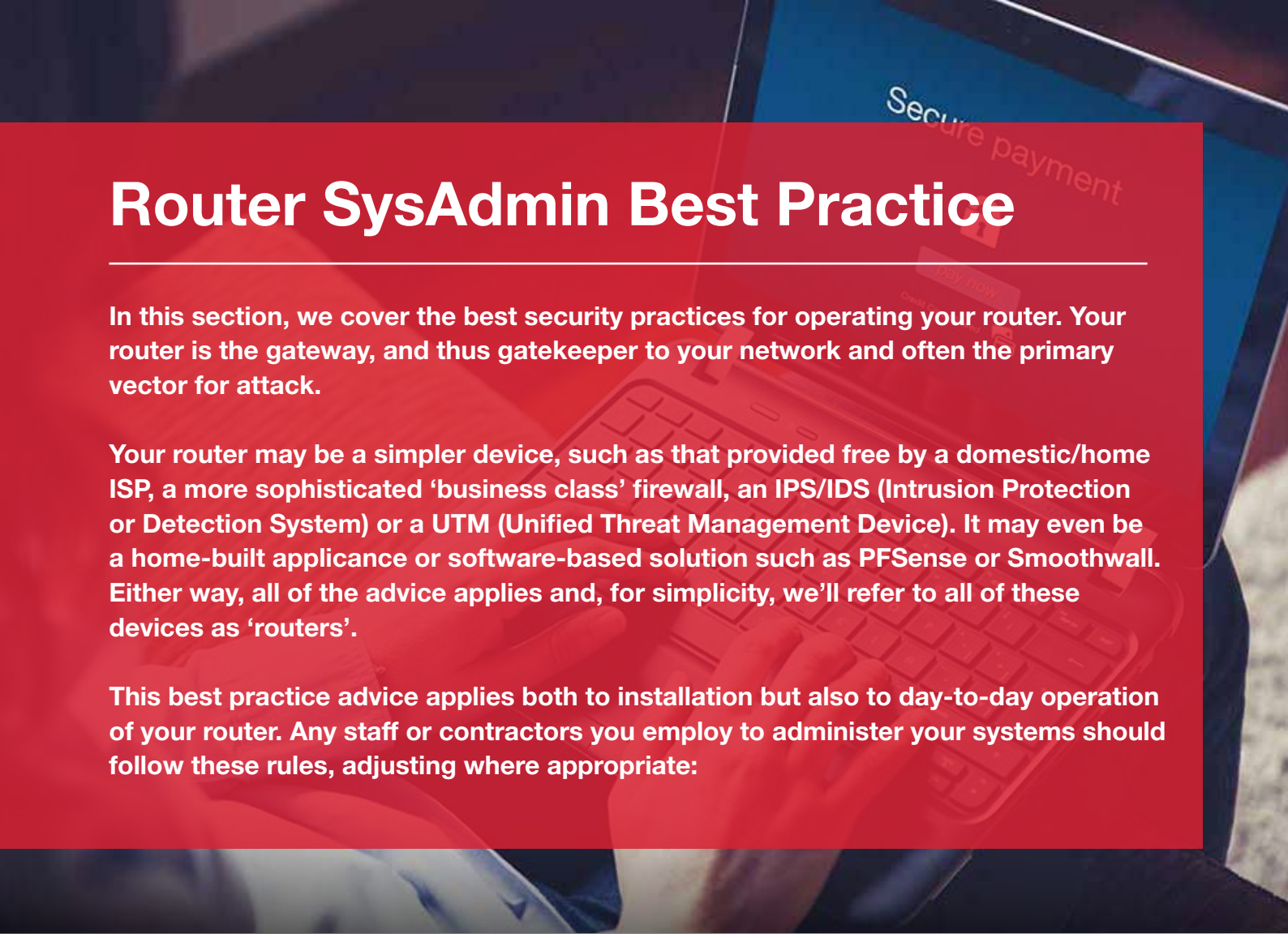
In this guide, we list some of the most important 'best practices' for operation of your router. It's easy to assume that a router comes out of the box with all security enabled – that is true to some extent with most products, but they will always be generic settings so you can improve that security and reduce the chances of becoming a victim by individual assessment.

You should adopt these practices as standard, adjusting and adapting them as appropriate for your own specific circumstances. No network can ever be 100% safe, but adopting these rules significantly reduces your vulnerability and demonstrates to your customers, suppliers and staff that you take a responsible approach to security.

We recommend you read this whole guide, even if just to confirm that you 'know it already'. Chances are you're already following many of the recommended precautions. As we said, your own circumstances and hardware will vary so this guide can't be exhaustive, nor will all of the recommendations apply to every installation.

Finally, it's worth reiterating that although this guide is published by DrayTek, these recommendations apply to all brands of broadband routers and wireless devices, so whatever vendor you've chosen, we hope you find the information in this guide useful.

"Most hacks, even some of the high profile, damaging incidents are not the result of brilliant hackers, complex methodology or obscure vulnerabilities, but merely exploiting failures to implement the most basic security precautions and best practices. Ensuring staff awareness of social engineering risks should also be a priority."



Router SysAdmin Best Practice

In this section, we cover the best security practices for operating your router. Your router is the gateway, and thus gatekeeper to your network and often the primary vector for attack.

Your router may be a simpler device, such as that provided free by a domestic/home ISP, a more sophisticated 'business class' firewall, an IPS/IDS (Intrusion Protection or Detection System) or a UTM (Unified Threat Management Device). It may even be a home-built applicance or software-based solution such as PFSense or Smoothwall. Either way, all of the advice applies and, for simplicity, we'll refer to all of these devices as 'routers'.

This best practice advice applies both to installation but also to day-to-day operation of your router. Any staff or contractors you employ to administer your systems should follow these rules, adjusting where appropriate:

1. Always change default passwords for router admin (on a DrayTek router the default is admin/admin). Changing the default password is the first thing you should do on any new installation. On some products, you can also have multiple admin logins so that each admin can use their own password which can be useful for auditing access.

2. Your chosen admin password should be 'strong' as should all other passwords on your router, including those used for SIP/VoIP accounts, IP PBX extensions and user accounts. Do not use the same password on more than one router. See 'Passwords' later.

3. Always specifically log out of your router's admin interface (web or telnet) when you have finished using it – don't just close your browser window. On most routers there is a 'Logout' button at the top of the web interface page. There will also be an equivalent telnet command if you are using the command line. Doing this gives additional protection against clickjacking and XSS attacks.

4. Do not enable remote management, TR-069 or SNMP on your router if you don't need it, and if you only need it temporarily, remember to disable it after use. Do not send syslog, SNMP or other logging data across the Internet (except within a VPN).

5. For administration of your router, always use SSL/SSH whenever possible instead of plain unencrypted access. For example, in your browser your router's IP address should be prefixed with https://. You can then disable regular unencrypted HTTP/Telnet. That provides much greater protection from snooping, especially if you are administering over a public connection or across the Internet. For remote admin access, you can use a VPN.

6. If you are using remote administration, restrict remote admin to known/specific remote IP addresses if your remote management is always going to be from known/fixed locations.

7. Monitor for suspicious activity. Using the various logging facilities of your router, and status displays, you may spot anomalous access or traffic patterns.

8. Always keep firmware up to date. All current routers undergo continuous development and new threats are evolving all of the time. New firmware may introduce new features but also essential security improvements and fixes.

9. Isolate any parts of the LAN from each other which do not need to communicate with each other by the use of VLANs. Use wireless LAN isolation is appropriate (WLAN-to-LAN and also client-to-client isolation).

10. Limit who has administrator access to your router (or other network components). Some devices also allow different logins for admin vs. other users and may also support logging of all admin access/activity so that you have an 'audit trail' of admin activity.

11. Disable any protocols not needed, in particular VPN (IPSec/PPTP) used for remote access, uPnP and WPS, leaving only those enabled which you actually need to use.

12. There are settings which you can disable but their effectiveness or risk varies and some will be at the expense of convenience Some settings to consider include disabling DHCP, ping and hiding your wireless SSID. In each case, these can improve security by reducing your attack surface but you have to consider you own requirements.

13. Have a published 'AUP' (acceptable usage policy) so that staff, visitors or household members know what is permitted on your network and what best practices they should adopt themselves in using it (for example not giving out wireless passwords to visitors too freely or writing passwords down). This should include specific rules about what email can be used for and common traps/risks to avoid – with email, but also any other web and Internet access.

14. For any remote or mobile access to your network, consider ‘two factor authentication’ (2FA). Instead of using just a single password, 2FA requires that you log on with a password and ‘something else’ (hence ‘two factors’). That might be a temporary PIN generated by a device or an app on your mobile phone. In this way, if someone obtained your password, they would be unable to log in - they would also need the other device or your PIN code. Your router may support 2FA; its use is a choice of a little extra inconvenience vs. increased security so its use depends on your own specific requirements. One-Time Passwords (OTP) are generated by a device in your possession (again, such as your mobile phone). The one-time password expires either after a couple of minutes or as soon as you use it so a key-logger (for example) on a PC would be useless in logging useful passwords.

15. If you use VPNs with your router as the endpoint, consider restricting access to specific local devices or separate subnets on your LAN if not everyone needs access. This may be particularly relevant for teleworkers who may wish to protect their corporate or head-office LAN from other household members’ or guests’ more risky devices/activity which could compromise your LAN.

16. Change any default security certificates. If you are using SSL/TLS (or HTTPS access) for any router functions (as you should be), give your router a unique security certificate, if possible, rather than the default one it ships with. Some routers will automatically generate a new unique certificate when first installed or upgraded. You can normally choose either a self-signed or CA-issued certificate. It’s important not to use the default certificates because if that is compromised (e.g. the private key is leaked from the vendor or reverse engineered from the firmware) then every user using that product is then vulnerable – their encrypted data can be decrypted.

17. Consider physical access to your network; the router, switches and other infrastructure. Avoid live RJ45 outlets in unattended places which may be accessible to the public or visitors. If network connected equipment is installed in unattended locations, consider securing or hiding the network cables. Consider additional wired client security such as 802.1x to prevent unauthorised devices from connecting to your network. Some Ethernet switches will alert you (or block) if unrecognised devices are connected.

18. If you ever need to provide temporary access to your router to anyone, for example temporary support staff or vendor's technicians (support departments), or if you send them your configuration backups for examination, set temporary passwords for them to use, or change the password after they have finished their work.

19. Subscribe to owners' mailing lists for your vendors. Should a vulnerability or exploit ever be identified, their mailing list may carry details of the appropriate remedy/update.

20. When making use of any features of your router which have selectable methods, always select the most secure protocol, where possible. Many of the older protocols are now considered flawed or of inadequate strength. For example, use IPSec/AES in preference to PPTP/DES, SHA-1 rather than MD-5 and WPA2 instead of WEP/WPA (for WiFi). Protocols such as PPTP, WEP and WPA are considered insecure nowadays.

21. Ensure that your router's real time clock is set correctly and to refresh itself with a reliable and trusted NTP server (public time server) in order that logs are accurate and that all scheduled events take place at the intended time.

22. Rogue DNS services (for domain/web address resolution) are used to redirect your web traffic without you realising. Only ever use known/verified DNS servers on your routers and devices. That means use the DNS servers provided by your own ISP or a trusted public source such as Google's (8.8.8.8 and 8.8.4.4). Your devices/PCs will often use your router as their DNS server, which in turn acts as a proxy to the public DNS server.

23. Only ever use new firmware and admin tools downloaded from your manufacturer's official web site – never from 3rd party sources (unless approved by your manufacturer).

24. If your router provides file-sharing, NAS or USB storage features, disable the feature if you do not need it (it should be disabled by default) and if you do use it, ensure that it uses strong passwords for access.

25. Keep backups of your router's configuration. Keep them securely and take new ones whatever you make material changes to your configuration. This will always enable you to return to a 'known working' configuration or save a lot of time if you need to replace or reset hardware.

Wireless LAN (WiFi) Best Practice

Wireless LAN (WiFi) provides businesses, homes and so many other locations great freedom and convenience, but that ubiquitous ease of access can also be available to unwanted users or actions.

There are many potential attacks possible against an insecure network. No matter how good your wireless router or access point is, failure to operate it correctly and adopt appropriate policies could leave you wide open, just like failing to use high security locks you might fit to your home or office.

In this section, we summarise the most important practices that anyone, homes or businesses, should adopt on a wireless network as well as advice for using a wireless device on someone else's network, or a public wireless service (such as in a coffee shop, airport or hotel).

1. Even if you are not using wireless but your router or network is wireless-equipped, change your access point's/router's wireless password from the default. If you have no use for wireless access, disable the feature altogether.

2. Use the strongest wireless encryption available. Although your router may support older security methods such as WEP and WPA, they are relatively easy to crack nowadays. You should use WPA2/PSK wherever possible or other stronger methods.

3. Consider setting an automatic schedule to disable wireless LAN during certain hours, for example overnight when your office is closed.

4. Change the default wireless SSID name and use a name that doesn't too easily identify your personal identity, company, location or the brand of router/access point, except for isolated guest wireless access where a recognisable name is generally expected

5. Create an isolated guest network. Create additional wireless and wired networks which are isolated from your private wireless traffic and your company network. This should also be used by staff when using their own devices for personal use (smartphones, tablets etc.). The guest network should be on a separate subnet and VLAN in order that it's impossible to reach your private network.

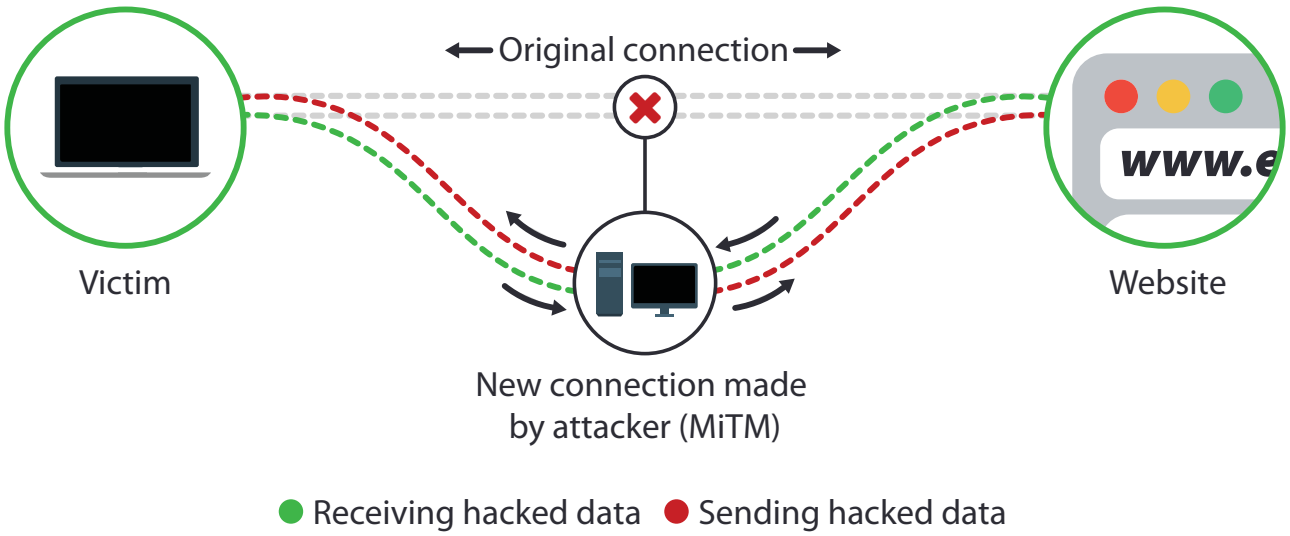
6. If you do set up a guest network/SSID, guests' devices should not be allowed to communicate with each other (unless you specifically want to allow that). On DrayTek routers this is called 'Isolate Member' in wireless settings but it may have different names on other brands.

7. Change your passwords periodically. Don't keep the same wireless password for years, especially if you have regular changes of staff or temporary workers.

8. If you let staff or guests access your network and therefore need the wireless password, then that also means that uninvited users can also get access. Staff and household members may not realise the implications of giving out the password just so that a guest can 'check their email' or whatever, so as well as a published AUP (Acceptable Use Policy) for staff, make use of your routers additional security features such as whitelists, 802.1x or MAC locking.

9. If your router is physically accessible, disable WPS. WPS is a convenient way to connect wireless clients to your access point or router and can also remove the need to divulge your wireless key (depending on the implementation), but that convenience may also be a security risk if an unauthorised person can press that button too.

10. **When using public WiFi, be sure about which network you are using, or meant to be using to avoid logging onto impostors/honeytraps. Anyone can set up a wireless connection called "Free Public WiFi" to attract victims. Any network operator can intercept your data; the possibility of MiTM (man-in-the-middle) attacks is always present, even when using encryption.**



11. If you use wireless LAN (WiFi) in someone else's home, office or a public access point (train stations, coffee shops) remember that the network owner and other users of that network can sniff/capture your traffic even if WPA encryption is in use (because they know the key too!). Use encrypted methods (e.g. SSL, HTTPS, VPNs) for all sensitive data. You can create a VPN back to your home/office router, or use a public VPN service and send all data down the VPN rather than directly via the guest network.

12. Many wireless devices (phones, tablets) will now store wireless passwords and back those up to the cloud. That's convenient if you use multiple devices or need to restore a configuration but this also means that Google (for Android), Apple (for iOS), Microsoft (for Windows) now have the wireless password for probably the majority of wireless LANs in the world. That's useful if you're a national security agency and want to spy on suspected criminals but if that information falls into the wrong hands (your competitors, hostile foreign governments etc.), perhaps by a rogue operative within one of those entities then it's potentially a big problem. Therefore, if you have sensitive company data, short of prohibiting wireless access altogether, consider not storing/saving WiFi passwords on devices, which requires cooperation from your staff.

13 Windows 10 has a feature called 'WiFi Sense' which enables you to share WiFi passwords with your contacts. It's enabled by default – consider disabling it unless you actually want to use it. Generally, be aware of what your O/S and apps/software are logging, storing and sharing with their suppliers (whether desktop, phone or tablet).

14. Use any diagnostic tools that your WiFi facility provides, for example lists of connected devices or traffic volumes to check that there aren't lots of unrecognised connections, indicating that you have a security problem.

Password Best Practice

In the previous two sections, we have variously referred to ‘strong passwords’. As these are so vital, this section explains what we mean by a ‘strong’ password and why you should use them. Even beyond your router, the use of strong, unique passwords is absolutely vital for all services, including online banking, ecommerce, but also any administration accounts you have on other hardware.

So much of your online activity relies on secure or controlled access and much of that will be password protected. Access to your router’s admin/configuration interfaces, including web and telnet are all password controlled. As your router is a gateway to your whole network, it’s clearly vital that it is protected with a suitable password.

Looking After Your Passwords

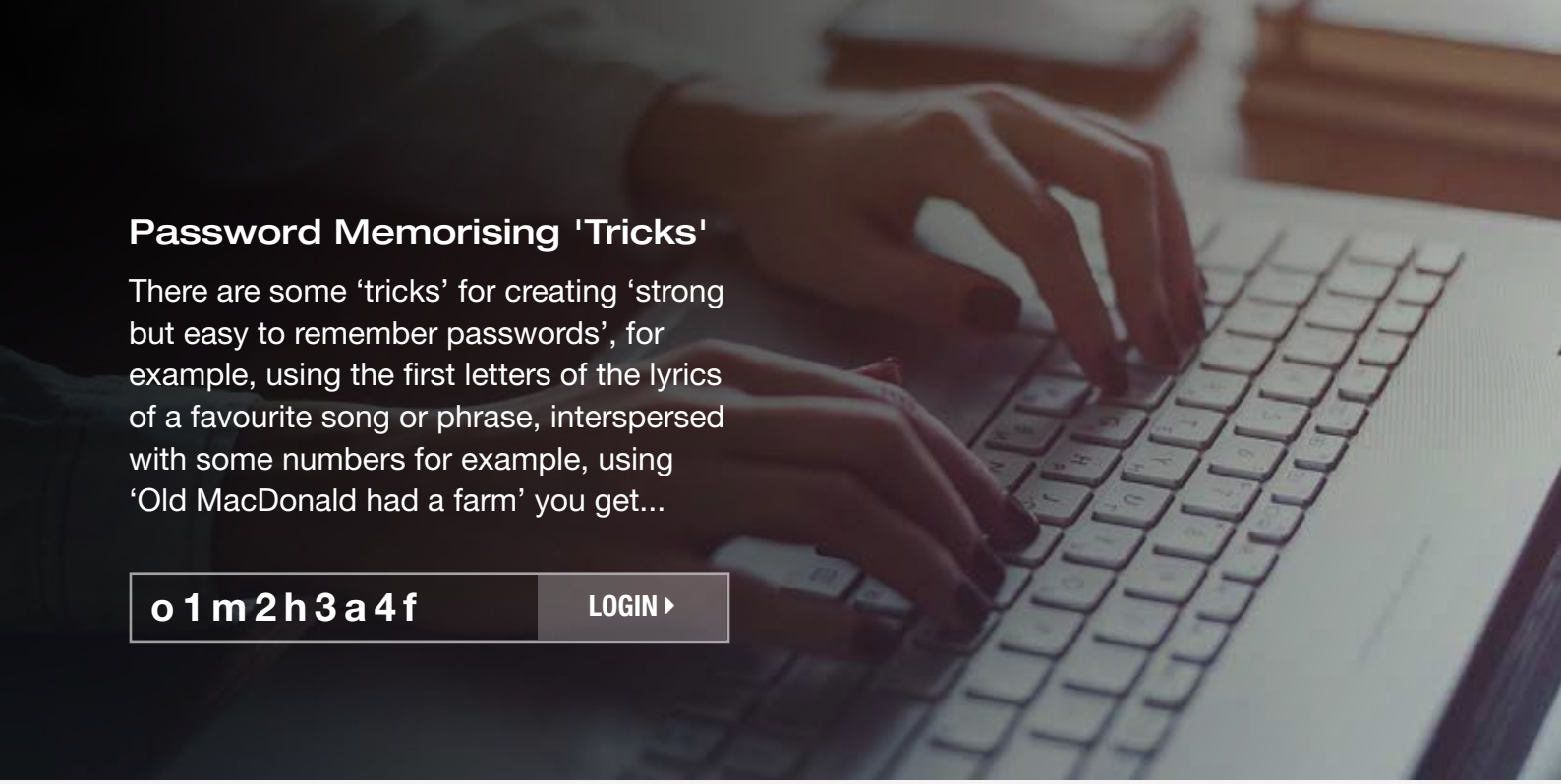
Passwords should be tightly controlled and divulged on a need-to-know basis only. For example, if you are setting up a staff member’s router for VPN access from home, they do not necessarily need to know the VPN password - you, as SysAdmin, can put it in for them. This isn’t suitable in larger enterprises where sysadmins should not know user’s passwords – again it’s all about an appropriate security plan for the specific environment.

Ironically, if you make user account passwords, which are expected to be manually typed, too strong, you make it more likely that users will write them down, so you can’t make manually typed passwords too strong - you will have to make a balanced judgement on how strong is ‘too strong’ for the purposes of annoyance.

Do not use the same password for different devices or services - each should be unique, otherwise if one service has weak security and is compromised, the hacker can then try the revealed password elsewhere. You should not use a common pattern. For example if you use ‘ebay1234’ and ‘amazon1234’ then it’s easy for a hacker to guess that you might also use ‘twitter1234’).

Users should never share or tell anyone their passwords. Users should fully understand that Sysadmins/tech staff will never ask for their password and they should never give it to anyone. This is particularly important to avoid imposters and social engineering attacks.

Users should be assured that they will never be reprimanded for refusing or challenging anything if they believe that it is contrary to security policies, even where they are led to believe that someone or the company will have great problems if they do not co-operate. In larger companies, staff should always challenge or confirm the identity of anyone who claims to need access to their systems, especially if the visit or call is unexpected.



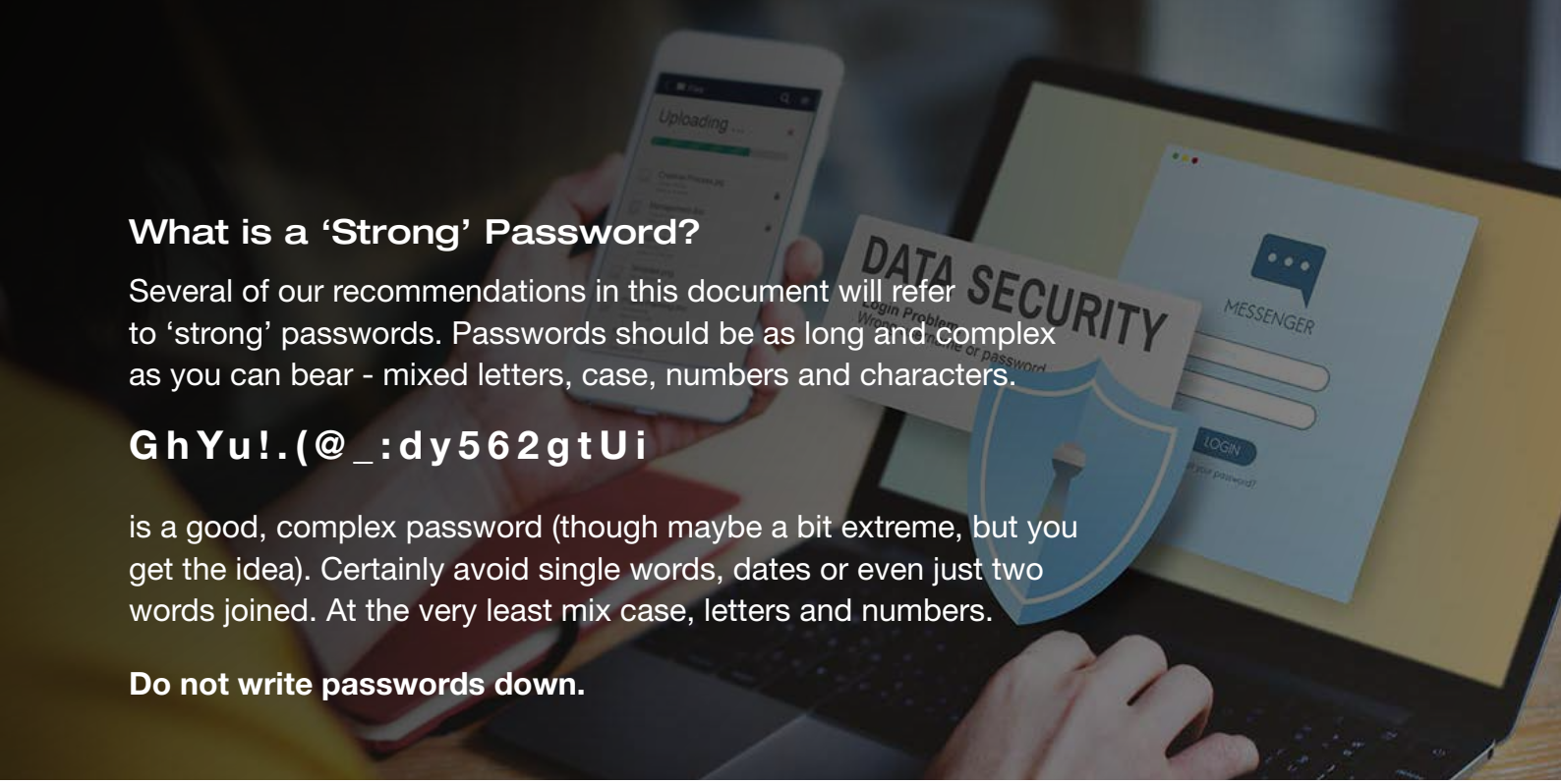
Password Safes

Most of us now have too many passwords to remember. As we’ll explain later, you must not be tempted to use the same password for different services/sites – passwords must be unique. Use a ‘Password Safe’ which is software or an app which lets you store passwords and other secrets in a database which is strongly encrypted. There are password safes available for every OS and mobile platform. Select one with the recognised/respected pedigree or one of the respected opensource projects. Access to the password safe is protected by one master password which you enter any time you want to open the safe. That master password must be very secure, not shared and, obviously never write that one down - keep it in your brain.

Unique Passwords

Unique passwords are vital; i.e. a different password for each different service, platform and provider. It is inconvenient, but if one service is compromised (hacked or data stolen in some other way), miscreants can then access your other services. Knowing that many people do use common passwords, hackers will try your password from one service on other services.

The problem with shared passwords was demonstrated in 2014 with the Heartbleed vulnerability. Sites which weren’t affected still had to advise their customers to change/reset their passwords if they had used the same password on sites which had been vulnerable to the Heartbleed exploit. Also, not all service providers operate the same security – it is standard practice to encrypt passwords as a ‘one-way salted hash’ but even now in 2016, some service providers still don’t do this, as demonstrated by some recent large-scale hacks



What is a 'Strong' Password?

Several of our recommendations in this document will refer to 'strong' passwords. Passwords should be as long and complex as you can bear - mixed letters, case, numbers and characters.

GhYu!.(@_:dy562gtUi

is a good, complex password (though maybe a bit extreme, but you get the idea). Certainly avoid single words, dates or even just two words joined. At the very least mix case, letters and numbers.

Do not write passwords down.

Summary of Router Related Passwords

The router administration password is the most obvious password in the context of this document, but there are many others you use. This is a summary of the most common router-related passwords. You will, of course, have countless other passwords for other sites (social networks, ecommerce etc.), each of which should also use a strong and unique password.

- Router admin passwords (for Web/terminal access)
- Wireless LAN Encryption passwords
- SIP (VoIP) account passwords (admin and endpoint passwords)
- VPN Passwords (pre-shared keys, site to site and teleworker)
- MyVigor (DrayTek account administration)
- Support portal and forum passwords
- TR-069/SNMP and other network management passwords
- LDAP/User Access/Accounts Passwords
- SIP Trunk Passwords
- Internet Access (ISP) passwords
- DDNS & SMS Service passwords
- Email (SNMP/IMAP/POP3) Passwords

Are Passwords' Days Numbered?

It is suggested that passwords themselves are really just SBO (see below); that people's propensity to share passwords, use weak passwords or otherwise be careless will always provide hackers with a reliable attack surface. Two-factor authentication (2FA) where, typically, a password and 'something else' is required is always stronger because even if a hacker has or guesses your password, they still need the other matching factor (for example a PIN generated by a device, or a digital certificate). Two-factor authentication may become standard within a few years making the single password obsolete. Many popular services already offer 2FA

Security by Obscurity ("SBO")

There is a common, often argued adage in computer security that "security by obscurity isn't security at all" which basically means that hiding things or making them harder to find isn't 'security' and you need to use 'proper' security methods. Those condemning security by obscurity ("SBO") point out that any determined hacker can easily bypass such measures, and recommending their usage might give you a false sense of security.

Of course, it is true that obscurity isn't security in itself, but making targets more cumbersome to attack and putting extra hurdles in the way can reduce the chances of an attempt because an attacker will more easily attack another target or may simply not allow for every variation because there are adequate easier targets.

An example of SBO is disabling DHCP – that is not security, but it does give an attacker one extra hurdle to overcome, which an automated attack may not bother with. The same applies to switching from router default private IP ranges. If CSRF (Cross-Site Request Forgery) attack code is hardcoded to attack LANs with the common 192.168.1.0 subnet, or at least starts there, using some other subnet range can prevent or slow the attack. Of course, you have to weigh up the inconvenience of the methodology against the benefits – for example, disabling DHCP might be hugely inconvenient for many networks.

Watch out for obsolete technology

Technology is constantly evolving. Today's high security and 'gold standard' of encryption is tomorrow's vulnerability. This happens due to the increase in processing power available to regular users. When DES encryption was introduced in the 1970's it was considered uncrackable with its 56-bit key. Brute force attacks of a 56-bit key are feasible with today's affordable computers. Tunnelling protocols like PPTP didn't even include encryption originally because it was introduced when networks weren't accessible over a public Internet or the risk and awareness of hacking wasn't really recognised. There's also WEP encryption for your WiFi – that was obsoleted by WPA, which itself was obsoleted by WPA2.

SSL is another technology considered obsolete. Note that we're talking about the specific technologies called to SSL (such as SSL 3.0) but the term "SSL" is often generically used to refer to encrypted web/Internet traffic such as HTTPS pages which mostly now use TLS1.2 encryption method. In 2014, a vulnerability (called Poodle) in TLS was discovered whereby a client could be tricked into falling back to the (insecure) SSL 3.0 protocol. The solution was that all major browsers issued updates which disabled SSL 3.0 altogether.

The takeaway here is that your router or other technology may support various protocols to allow for backward and 3rd party compatibility but you should always use the most secure protocols available (taking into account performance considerations and risk) and disable any protocols not needed (e.g. WEP/WPA for WiFi). Another example: if you set up a VPN connection, disable all methods which are not needed.

Don't Ignore IoT

In a 2016 survey of security publications and web sites, the most commonly predicted new front for attack was IoT – the Internet of Things. That's the new wave of connected devices in your home or office – doorbells, fridges, heating, lightbulbs, AV and so on. This is a huge exciting growth area for technology but much of it is immature and it seems that in the rush to be first to market, security considerations are often lower on the priority list than they should be. Just like your PCs and networking hardware, your IoT devices should communicate securely onto the Internet and should use passwords for control and access – ask your vendor if yours does. It's not just small things – even Internet connected cars have had vulnerabilities exposed.

Check that your vendor is committed to regular updates to patch vulnerabilities and will continue to support the product.

Anti-virus Still Matters

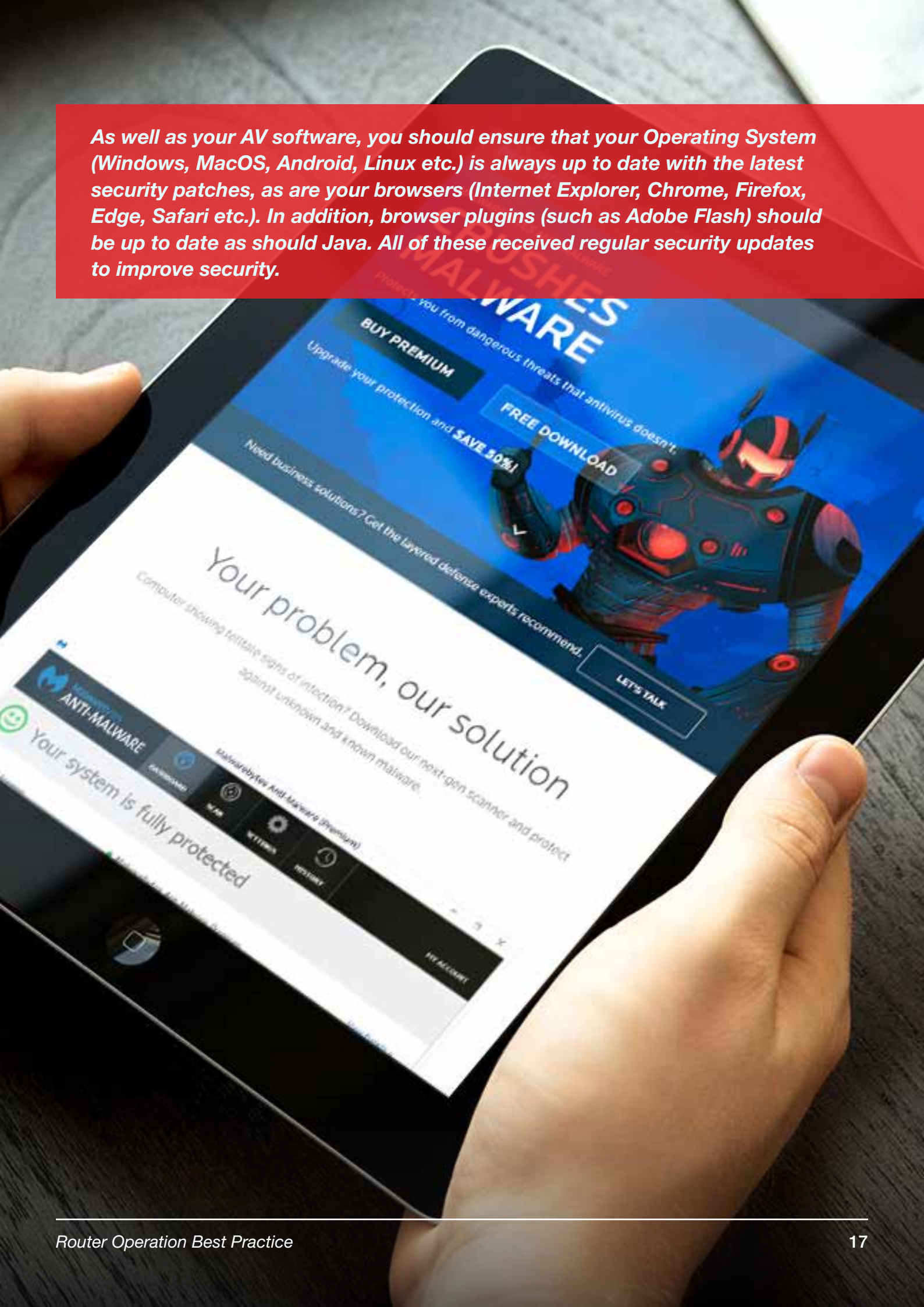
With all of our focus on hardware security, it's important to remember the importance of every device still being equipped with competent, up-to-date anti-virus (AV) software. AV software is available for all platforms, including mobile - and indeed, your mobile phone can be infected just like a desktop PC. Maintaining and using AV technology is especially important as the sophistication and insidious nature of viruses and trojans is greater than ever (a Trojan is a virus hidden inside something innocent looking, as in the Trojan Horse). The most common types of virus can be DoS zombies (relays), Spam zombies, keyloggers, data thieves, ransomware (see later) or keyloggers.

A 'zombie' is a normally sleeping program, waiting for instructions from a commander elsewhere on the Internet. By using tens of thousands of zombies, the command centre can rapidly transmit vast amounts of data from vast numbers of locations towards a target, overwhelming the target victim's connectivity (thus denying them service). This is known as a Distributed Denial of Service (DDoS) attack. As the attacks are coming from thousands of locations, which are themselves not responsible for the attack, it's impossible to stop the attack (but it can be mitigated against). A zombie may also be used as an email relay to send spam or phishing emails, making it untraceable.

The more recent combination of social engineering and viruses means that it's easy for even the most seasoned professionals to be fooled by an email or USB stick/CD which looks innocuous or legitimate, and you then get infected. Viruses are most commonly contained in 'office' documents or executables ("Please find your invoice attached...") but even PDF files can have rogue content. Control your curiosity if you are at all suspicious; always be alert.

You can sometimes check email headers to expose a forged source, though if the virus was sent from an infected known contact even the header will look legitimate. If you're not sure about an email attachment from a known person, err on the side of caution. If it's from an unknown person, run away – delete the attachment – do NOT be tempted to open it and hope your AV software will catch it.

Even with AV software installed, a new or mutating virus may not yet be recognised by your AV software yet so it's vital to reduce your chance of being infected. Best practice in relation to email attachments and visiting compromised web sites is essential. Your router/firewall may provide content filtering services which will block compromised web sites in real time, however only once the compromise has been recognised. The most common compromised web sites are those that appear to be offering something for nothing.



As well as your AV software, you should ensure that your Operating System (Windows, MacOS, Android, Linux etc.) is always up to date with the latest security patches, as are your browsers (Internet Explorer, Chrome, Firefox, Edge, Safari etc.). In addition, browser plugins (such as Adobe Flash) should be up to date as should Java. All of these received regular security updates to improve security.

Backups & Ransomware

Backing up your data is old, but good advice and in itself beyond the scope of this document, but with the growth in ransomware, it's more important than ever.Ransomware is a relatively new phenomenon where a virus will silently encrypt all of your data and once done, pop up to demand payment to unlock it. The criminals typically demand payment in untraceable Bitcoin and there are examples of bugs within ransomware preventing decryption even when the ransom has been paid, or the criminals just taking the money and not providing the encryption keys. The effect of this has been immense on some victims in both large companies and private individuals. Imagine complete company data sets, or personal documents being lost.

With ransomware, preventing infection is obviously best (see previous section), but should the worst happen, you'll be glad of backups, though we'd hope that you were already backing up your data to allow for the more traditional risks (disk failure, hardware theft etc.). Your backups need to be regular, recent and offline. Each of those characteristics is vital:

1. You need the backups to be regular and recent, so that you lose the minimum amount of most recent data.

2. The backed up data needs to be 'offline' i.e. not stored on your PC or any device which your PCs (or other devices) have access to, as otherwise the ransomware can encrypt your backups too. If you keep your backups in the cloud, lock out that storage so that your PC (or other device) doesn't have directory access to it as otherwise the ransomware could encrypt that too.

3. You need to ensure you have multiple aged backups. If you keep just one backup, you might be backing up locked/encrypted data, overwriting a previous useful backup, so keep as many previous backups as is practical (for example the last 7 days' single backups, the last 4 weeks' single backups and the last 6 month's single backups.

Make Full Use of Your Router/Firewalls

Your firewall is, most likely, providing stateful protection of your LAN-side devices by default. This means that an external source (or attacker) cannot target your internal devices from the outside - your firewall will only pass reciprocal data, which is data received as a reply to an outgoing request. The router keeps the state of all external sessions (hence 'stateful'). Your router, however, can do more than just the automatic firewalling, notably additional IP filtering - that is setting up rules to block or allow traffic based on their source or destination addresses, or traffic type.

Consider setting up additional IP filters to block or permit access to specific destinations where devices do not need full Internet access. For example, an internal server which doesn't need Internet access, could have that blocked, other than for essential services (update sites for the O/S, anti-virus, cloud backup etc).

If you have IP CCTV cameras or IP phones on your network, block those from Internet access if they don't need it (you can just set a false gateway). If you are using VPNs, set IP filters so that the remote users only have access to the resources (e.g. specific servers) and protocols (e.g. just remote desktop) that they need. Block any other remote devices across a VPN from accessing your LAN if they do not need access.

You can block all devices on your LAN, other than mailservers, from sending email using the SMTP protocols (ports 25, 465, 587). That may prevent bots (zombies) from distributing spam from your network.

Much Internet traffic now uses SSL/TLS encryption. That also encrypts the web address or URL (e.g. www.google.com) so do be sure that if you are using any content filtering that your device is able to detect and block URLs which are being accessed through an encrypted connection.

Routers do also provide many other security features such as content filtering, Denial-of-service mitigation, time scheduling etc. and you should make appropriate use of those. Enable logging so that you can see if or how much those filters are being used. If you are using IPv6 remember that every LAN device has a public IP address - ensure that you are firewalling those with a default-deny rule (except for public facing servers, and then allowing only the necessary protocols).

Tor

Tor (originally called 'The Onion Router') is an anonymising service for Internet traffic. Tor provides anonimity to both users and services by relaying your traffic via multiple random relays until eventually exiting the Tor network to get to its destination (at an exit node). In this way, each end of the connection cannot trace or the origination point, so your IP address is anonymised. Tor can be used to access any regular web site anonymously.

Services can also exist inside the Tor network itself so they are not accessible over the regular Internet at all. Tor has its own DNS system for locating in-network services. The 'Dark Web' is the collective name for these in-network sites. The 'Deep Web' is a subset of those services which are secret/unlisted. The Dark Web is most famously used for services and users involved in illegal trade, including illegal pornography, piracy, hacking, trading stolen data, fraud-enablement and the sale of firearms and illegal drugs. Tor is also widely used by hackers. Not everyone using Tor is a criminal: Some people use Tor to speak out against oppression, say inside a particular regime where there would be consequences if they were identified, including whistleblowers, poltical dissidents or journalists.

Tor is a tunnelling protocol, and that provides a challenge for any company, school or home trying to control their network traffic or user activity. Tor packets look like standard HTTPS/ TLS (SSL) traffic, so are not easily identified. This means that if you have measures in place to help block certain services, a user may be able to tunnel through Tor and bypass those measures. Your organisation stands at risk of allowing access to illegal or offensive web sites or activities which you otherwise thought you'd blocked. A lot of malware is distributed via sites on The Dark Web (or Deep Web), sometimes in drive-by web site downloads and sometimes hidden in downloads.

You may therefore decide that you need to prevent Tor being used on your network. If you control all devices, you may be able to prevent Tor being installed in the first place, but where people can install software or use their own devices, that's not an option. Every Tor exit node has to be published, so you may be able to build an ACL (access control list) to block those (this needs to be regularly updated), or do real time queries against a live database. You may also be able to install a product which can run deep packet inspection or statistical analysis to recognise and block Tor traffic.

Above all, if you do want to ban Tor, remember the human element. Ensure that your users' AUP (Acceptable Use Policy) specifically prohibits the installation or use of Tor. If your staff know that it's strictly prohibited, they are far less likely to try to install it or try to circumvent blocks.

Conclusions & Summary

As an overview, this guide can never be fully comprehensive, nor can it cover the specific topology of your own network and environment but hopefully we have demonstrated that there are many simple precautions that you can adopt to markedly increase your security. This guide also doesn't cover the specific configuration and usage of the security features provided by your router. You should apply all appropriate measures and take specific advice from your security experts or study the manuals of your products.

On the subject of hackers, white-hat hackers are hackers who provide services to companies in testing networks' resilience and security as opposed to 'black hat' hackers who are the bad guys causing mischief, chaos, damage, theft, embarrassment or other loss. You may wish to consider hiring a white hat to 'pen test' (Penetration Test) your network/IT security, but do check who you're dealing with, be clear on their terms of service and NDA policies, take references and be clear on their remit.

You should conduct regular risk-assessments of all of your IT and users. This guide was produced by DrayTek – whose primary products are routers, so that's our focus here but of course, there is a lot more to your IT than just routers, wireless LAN and passwords. Every piece of IT equipment can be a point of vulnerability, even something as apparently benign as a printer.

Of course, even non-IT can be a point of vulnerability, such as door locks and windows. We're used to maintaining and assessing those regularly, so IT should be no different, but digital systems provide more opportunity for undetected misdemeanours so consider whether you have adequate (but proportional) means to detect and react to attacks. You should also consider what level of recording, logging or auditing is appropriate for your network – for example whether you should log all device connections, remote logins, DHCP services etc.It is actually more common that user's lack of care or insufficient risk awareness rather than deliberate misdemeanour leaves you at risk so adopting an appropriate AUP (see earlier) and making users/staff aware of the importance of prudent operation is vital.

Thank you!

Thank you for reading this guide; we hope you found it useful. Please do get in touch if you have any comments, corrections or suggestions – we genuinely welcome your feedback and please do recommend this guide to associates and colleagues - just send them to or tweet www.draytek.co.uk/best and help everyone have better network security.

Vigor 2860 Series

The Ultimate ‘xDSL’ Router

- ADSL2+, VDSL2 and broadband router/firewall
- IPv6 & IPv4 dual-stack
- BT SIN 498 MCT Approved
- Built-in dual-band WiFi & 802.11ac
- Comprehensive and robust firewall
- VPN site-to-site & teleworker connectivity
- Configurable QoS (traffic prioritisation)
- 6-Port Gigabit Ethernet Switch
- Content Filtering (by keyword or data type)
- 802.1q VLAN tagging & multiple subnets
- Twin phone ports for VoIP (Option)
- Managed Wireless for DrayTek APs
- Rack mountable (optional kit)
- Huge range of other features

VigorBX 2000ac IP FBX & Router/Firewall

Complete IP phone / call handling system

IP PBX features:

- Uses internet instead of phone lines so no line rental and low cost calls
- Up to 50 extensions (local or remote)
- Voicemail for every extention with phone or email delivery
- 2 Analogue line interfaces (FXO)
- Analogue phone port (FXS)
- Multi-level IVR (“Press one for sales”)
- Call groups and flexible call distribution
- ADSL2+ & VDSL Rouer/Firewall
- Built-in 802.11ac Wireless
- 6-Port Gigabit switch

Vigor 2860Ln with 3G/4G/LTE

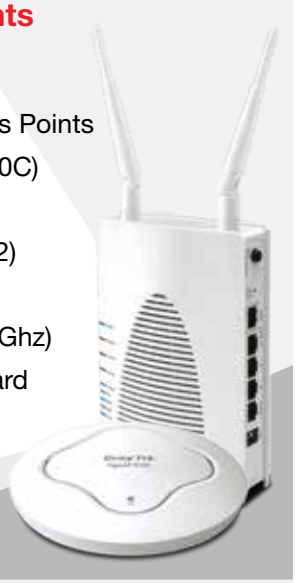
- Built-in SIM Slot
- LTE: Up to 150 Mb/s
- ADSL/VDSL built-in
- Text-message control
- Includes all other feature of the Vigor 2860 series

See website for details

AP 910C / 902 Access Points

Ceiling or Wall 802.11ac

- Business Class Wireless Access Points
- Ceiling or Wall mounted (AP 910C)
- Desk or wall mounted (AP 902)
- 4+1 Port Gigabit switch (AP 902)
- Latest 802.11ac technology
- Simultaneous duAl-band (2.4/5Ghz)
- PoE Powered (or DC) as standard
- Multiple security facilities



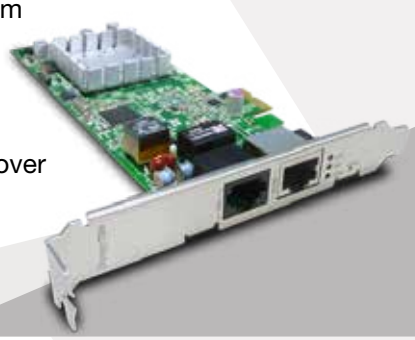
VigorNIC 132

PCI-e Card ADSL/VDSL Modem/Router

- Half-height PCIe card (½ plate included)
- Windows & Linux support
- Ethernet (RJ-45) interface
- Router & Bridge/modem
- ADSL/VDSL interface

Ideal for

- WAN Redundancy/failover
- Software Firewalls
- IP-PBX Installations



VigorSwitch

Gigabit & PoE Switches

- Gigabit smart or L2 Managed
- 8 or 24 Port full power PoE

PoE models to power:

- Access Points
- IP Cameras
- IP Phones

Vigor 2952 / 3220

High Performance Routers

- 2 or 4 Gigabit WAN Ports
- Load-balanceing & failover
- 500Mb/s Performance throughout
- standard DrayOS OS/interface
- 30-node wireless management
- Internet content filtering
- 100 IPSec VPN Tunnels
- SSL VPN

DrayTek Managed Wireless

DrayTek's new managed wireless facility is built into several of our router models. - Just add DrayTek wireless access points and your users and guests can have reliable coverage and optimised performance, whilst you have control, security and comprehensive monitoring.

- No dedicated/specialist controller required
- Mobility - Wireless throughout your premises
- Load-Balancing across multiple APs
- Reporting, logging & monitoring
- Security & isolated guest access

Visit: www.draytek.co.uk

DrayTek

@DrayTekUK

info@draytek.co.uk

www.draytek.co.uk

DrayTek UK

2nd Edition updated 10th July 2016. The next page is an advertisement and not part of the guide.