KONICA MINOLTA

workplacehub

SECURITY TOOLKIT FOR SMBS

HOW TO MAKE SURE YOUR SMALL BUSINESS IS PROTECTED

2020 EDITION

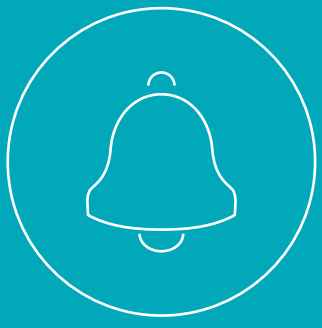
Giving Shape to Ideas

97%

OF BREACHES HAD AN IMPACT LASTING MORE THAN 24 HOURS

1 IN 8

CYBER ATTACKS ARE SUCCESSFUL



78%

OF BUSINESSES TAKE 7 DAYS OR MORE TO DETECT SECURITY BREACHES

CONTENTS

1 ESSENTIAL CYBERSECURITY SOLUTIONS FOR SMBS

The 5 key areas you need to have covered to make sure your SMB is protected.

2 HOW TO SPOT A CYBER SCAM

What this means and the red flags to look out for.

3 CYBERSECURITY CHECKLIST

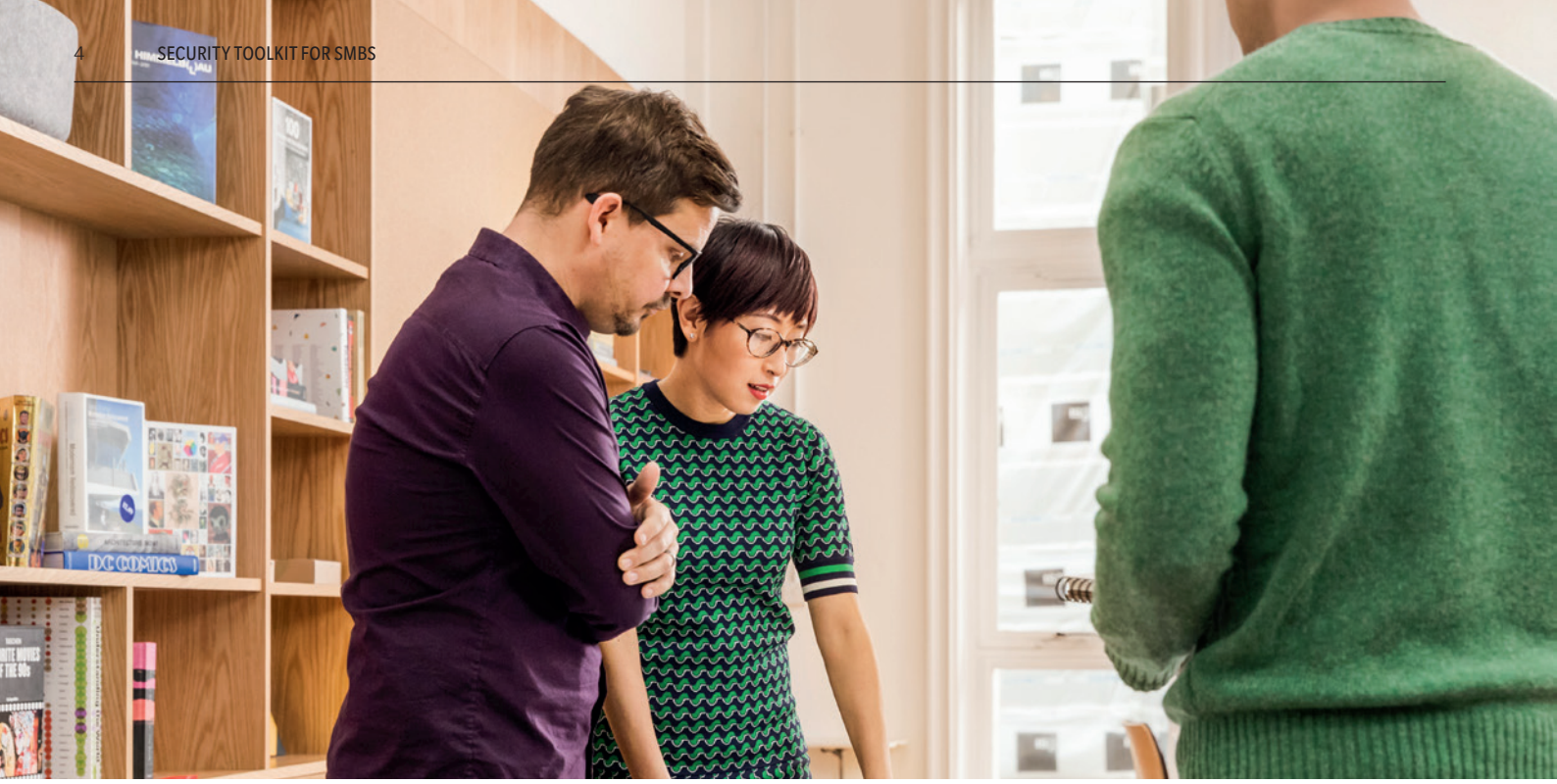
An easy list to work your way through and make sure you're doing everything you can to look after your business.

4 QUICK WINS ACROSS YOUR IT

5 areas where you can make some quick changes to get your IT working for you.

5 COVID-19 DRIVEN SECURITY CONCERNS

Addressing the new cybersecurity concerns that have arisen from the global pandemic.



ESSENTIAL **CYBERSECURITY** SOLUTIONS FOR SMBS

One in five of SMBs report using no endpoint security, and one-third of companies rely only on free solutions.[1] This leaves many SMBs at significant risk.

Here are 5 key areas you need to have covered to make sure your small business is protected.

PASSWORD MANAGEMENT

Weak passwords can be a prime entry point for hackers to take advantage of your systems – especially considering the fact that 83% of users surveyed by Cyclonis admitted to using the same password for everything![2]

To be able to create a strong password, these are the topcriteria to hit:

- Must be at least 8 characters long
- Should not contain any of your personal information – especially your real name, user name, or even your company name
- Must be very unique from your previously used passwords – no incremental numbers here!
- Should contain a mixture of uppercase letters, lowercase letters, numbers, and special characters

ANTIVIRUS SOFTWARE

This is where all cybersecurity starts. Designed to detect, block, and remove viruses and malware, make sure that your software protects against:

- Ransomware
- Keyloggers
- Backdoors
- Rootkits
- Trojan horses
- Worms
- Adware
- Spyware

[1] Source: https://www.prnewswire.com/news-releases/bullguard-new-study-reveals-one-in-three-smbs-use-free-consumer-cybersecurity-and-one-in-five-use-no-endpoint-security-at-all-301007466.html

[2] Source: https://www.cyclonis.com/report-83-percent-users-surveyed-use-same-password-multiple-sites/#:~:text=for%20Multiple%20Sites-,Password%20Security%20Report%3A%2083%25%20of%20Users%20Surveyed%20Use%20the%20Same,and%20child%20on%20the%20planet

FIREWALLS

A network firewall is essential to monitor incoming and outcoming traffic on your network. They basically separate your secure internal network from the insecure wider internet.

Top services to look out for in your firewall:

- Intrusion prevention services (IPS)
- Gateway antivirus (GAV)
- Content filtering
- Anti-spam features
- Application control
- Protection for non-standard ports
- Cloud sandboxing

PATCH MANAGEMENT

Believe it or not, outdated versions of software can expose your business to massive security risks. Cyber criminals design their attacks around vulnerabilities in popular software products – even from the biggest companies, such as Microsoft Office, Adobe Reader etc.

Generally, as these vulnerabilities are exploited, vendors will issue updates to address them – but if you don't have these turned on for automatic updates, or are guilty or pressing snooze one too many a time, you could be harming your business without even realising.

TOP TIP

Make sure automatic updates are part of your regular computer and network maintenance.

BACKUP & RECOVERY

If you do get infected by a virus, or lose access to your data due to uncontrollable incidents such as a fire, make sure you have a full offline backup of your system that is up-to-date and separate from the main network, so you don't have to start from scratch.

You can then reboot to safe mode, use anti-malware software to remove any malicious software, and restore your computer to a previous state.

TOP TIP

Backing up once a year won't cut it – have it scheduled regularly, and most importantly test it regularly. Otherwise, it might be that your only option is to pay up.

HOW TO SPOT A CYBER SCAM

Cyber scams (also known as phishing) are when cyber criminals impersonate brands, banks, vendors, even your own colleagues, to obtain sensitive information such as usernames, passwords, and banking details, or manipulate you into downloading malware or ransomware.

Cyber scams most commonly appear as emails with seemingly harmless email attachments, or branded as a company that you normally trust.

THE RED FLAGS TO LOOK OUT FOR:

Missing sender or recipient information

- Generic greetings
- Slight misspellings in email addresses
- Email addresses that don't match the company name
- Asking you to download or click a link from a sender you don't recognise

Nearly 40% of SMBs report losing crucial data during a cyber attack.[3] That data includes:

- customers' names
- personal addresses
- emails
- stored credit card numbers
- confidential business plans

REMEMBER:

Your business brain is now embedded in your data and should be safeguarded.

Another common scam to look out for are malvertising and pop-ups – adverts that either look legitimate but take you to an infected site, or that claim your computer has been locked / infected already, and that to regain access the user must click a link to pay a fee. Naturally, this is all a ploy to gain quick access to your banking details, but the fear of losing control of your personal computer can often be enough to override common sense.

THE RED FLAGS TO LOOK OUT FOR:

- Links that redirect to a different domain
- Pop-ups that require you to enter personal information
- Misspelled URLs
- Threats of any kind

[3] Source: https://www.prnewswire.com/news-releases/bullguard-new-study-reveals-one-in-three-smbs-use-free-consumer-cybersecurity-and-one-in-five-use-no-endpoint-security-at-all-301007466.html

CYBERSECURITY CHECKLIST

Still with us? Here's an easy list to work your way through and make sure you're doing everything you can to look after your business.

REVIEW YOUR DIGITAL FOOTPRINT

Attackers can take data from social media accounts, company websites, press releases and even company registration details.

Take a look at what information you have available online, reduce it where you can, and always be wary of a seemingly 'out-of-the-blue' request. There's no shame in reconfirming details from your side before agreeing to share anything – just remember to check it with your own sources rather than responding directly to an email or calling back the same number.

STAFF TRAINING

It's as simple as taking the time to make sure your employees are aware of what security risks look like: for example, how to recognise a phishing email, or how to flag a suspicious website. Continue to raise awareness within your business by implementing regular communications around the latest cybersecurity threats – if resource is limited, set up a Google Alert or subscribe to your favourite media outlet to get automatic notifications.

PROTECT YOUR HOME ENVIRONMENT

Password-protected home Wi-Fi networks are not safe from hackers! A VPN (virtual private network) for employees to connect to, and provide a secure link by encrypting data that is sent and received, is a great first step in securing your home office.

INVEST IN NETWORK AND INFRASTRUCTURE SECURITY

Implement a password policy that requires strong passwords that expire every 90 days, and deploy next-generation firewall, VPN and antivirus technologies to ensure your network and endpoints are not vulnerable to attacks.

REGULAR SCHEDULED MAINTENANCE

It is essential to use up-to-date software products and be vigilant about patch management – didn't you read the first section? And don't forget those daily or weekly data back-ups too, otherwise you'll be starting from zero should the dreaded data loss happen.

ILLUMINATE YOUR BLIND SPOTS

Choose security tools that proactively identify suspicious events – the focus should be on prevention rather than repair when it comes to security for your business. Not only does this minimise risk, it will show you where the attacks are getting in, so you can make sure they're plugged for the next time a criminal tries their luck!

LEARN THE VALUE OF REAL-TIME SANDBOXING

Cloud and / or network sandboxing services offer real-time inspection of suspicious files that firewalls and malware protectors aren't quite sure about, and quarantine any potential risks. In other words, it's advanced threat detection that you don't have to worry about.

QUICK WINS ACROSS YOUR IT

EMAILS

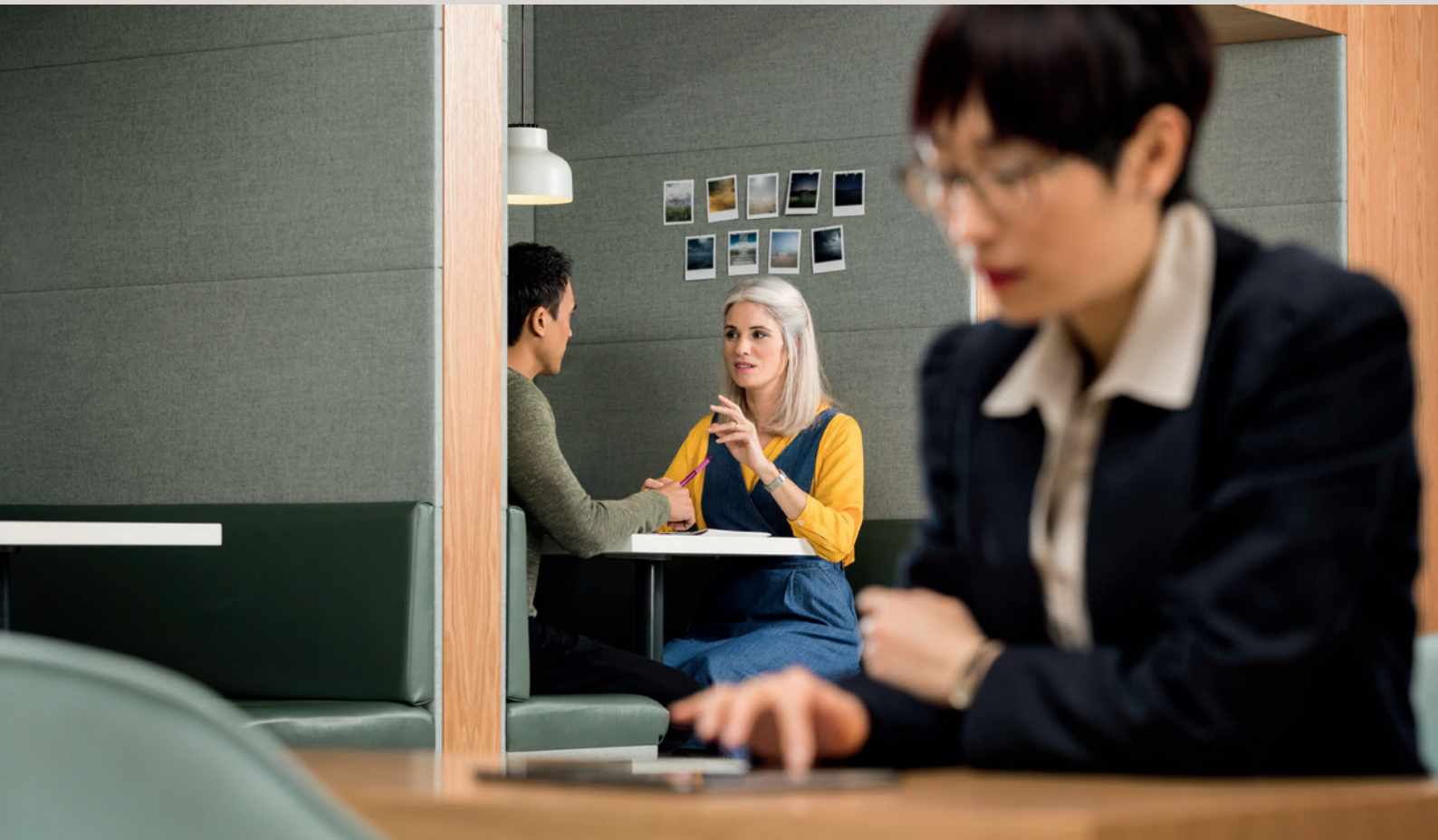
- Require strong, unique passwords on email accounts
- Turn on two-factor authentication if offered by yourprovider
- Ensure employees don't use personal email accounts for any company business
- Set up spam filters to capture any potential threats before they enter inboxes

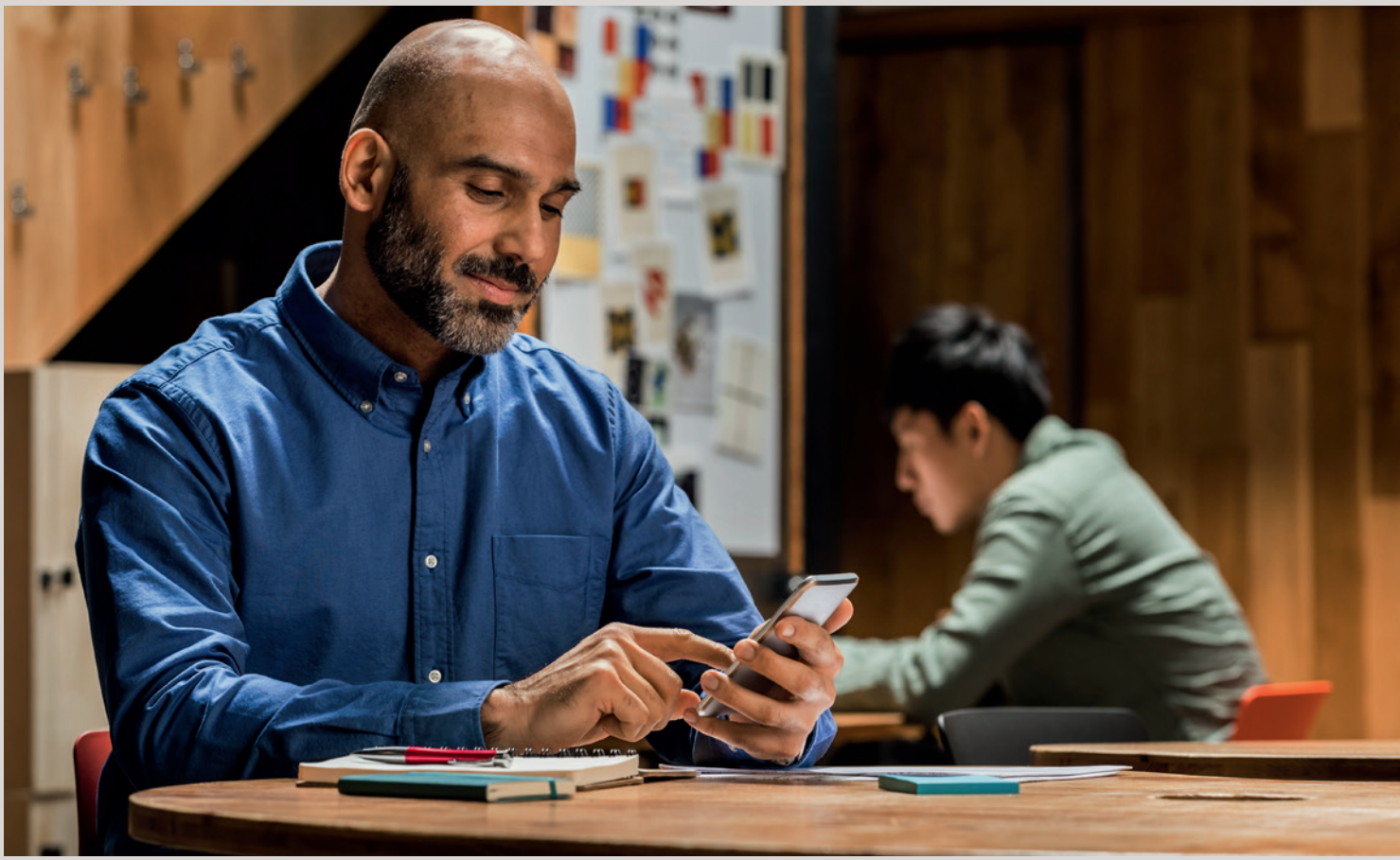
PRINTERS/SCANNERS/COPIERS/MFPS

- Change the default password to a strong and unique password
- Ensure devices have encryption and overwriting capabilities
- Digitize as much information as you can, and dispose of hard copies if no longer needed

FILE SHARING

- Provide a trusted, secure service for employees, and disable alternative, free services that don't provide legal protection
- Restrict the locations to which work files containing sensitive information can be saved or copied





MOBILE PHONES

- Ensure software updates are applied automatically and regularly
- Only download apps from a trusted source, and run anti-virus prior to running
- Secure devices with passcodes or other strong authentication, such as fingerprint recognition
- Activate “find device” and “remote wipe” settings

WI-FI NETWORKS

- Use separate Wi-Fi networks for guests and employees
- Use a virtual private network (VPN) when using public Wi-Fi
- Do not connect to unknown, generic or suspicious Wi-Fi networks - use your mobile carrier’s data plan to connect instead
- Secure your internet connection by using a firewall, encrypt information and hide your network

COVID-19 DRIVEN SECURITY CONCERNS

As COVID-19 continues to affect working practices in 2020, it raises new cybersecurity concerns for SMBs.

Working remotely and securely is not as simple as just taking your laptop and mobile device home. Beyond the traditional "office in a box" set-up, there is a pressing need to secure remote workers and balance employee privacy with corporate security standards.

With 78% of SMB employees temporarily working remotely, and an anticipated 56% suggesting some positions will be permanently remote moving forward, it's no surprise that over three-quarters of small businesses worry about their remote devices or remote employees being breached.[4]

ADAPTING TO CHANGE

As the abnormal becomes the next normal, SMBs need to approach remote work by using a combination of cloud-based applications and on-premises solutions to keep employees and systems safe, and ensure business continuity.

Look for technologies that incorporate:

- multi-layered network security tool
- a hybrid network infrastructure, such as SD-WAN
- proactive endpoint protection platforms and firewalls to avoid large-scale network vulnerabilities, regardless of budget and resource size.

BEWARE OF TARGETED ATTACKS

Experienced hackers are exploiting the COVID-19 outbreak to send fake emails to employees that appear to come from company officials, and ask you to open a link to a new company policy related to the pandemic. Commercial malware AveMaria jumped over 1,200% from January to April, an enormous increase from 2019.[5]

Upon clicking on the link or opening the attachment, you're likely to download malware onto your device and allow cyber attackers to take control of your computer, log your keystrokes, and/or access sensitive business information.

20% of businesses said they faced a security breach as a result of a remote worker. This, in turn, led to higher costs.

A LAYERED APPROACH

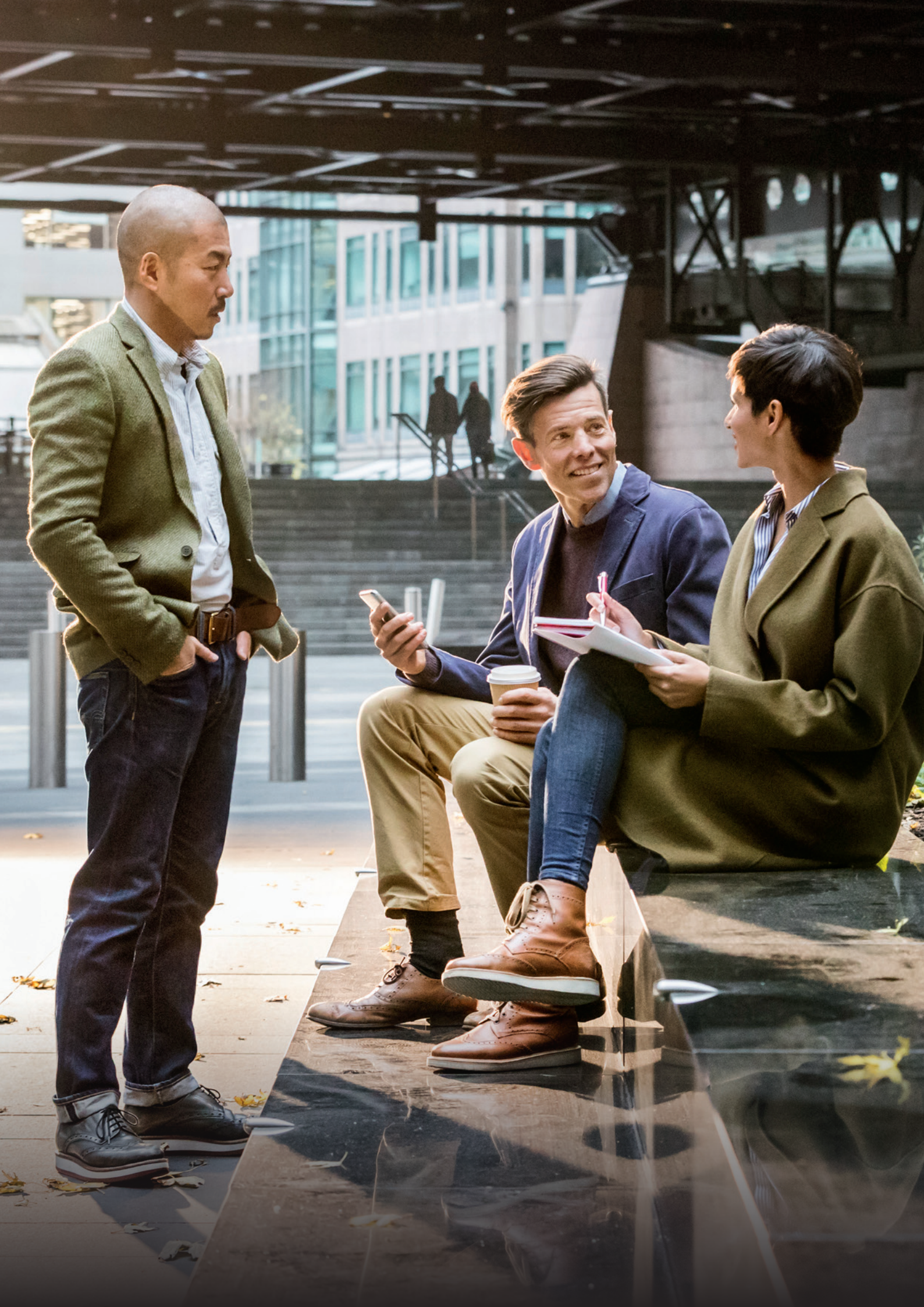
It's clear that workplace security is just as important whether you are in the office or working from home. To truly protect your home environment, make sure your business has a multi-layered strategy that covers areas such as security awareness training that tests each user; anti-virus solutions; data back-up; endpoint encryption; and a managed VPN/ firewall.

With that in place, you can rest assured that your business can operate smoothly wherever employees are located, and that your technology is available, productive, and protected.

One in four (24%) had unexpected expenses to address a cybersecurity breach or malware attack following shelter-in-place orders.[5]

[4] Source: https://www.connectwise.com/resources/smb-research?source=LND-PR-Article-PRWire-NA-2020&utm_campaign=earned&%20utm_medium=pr&utm_source=prwire&utm_loc=all

[5] Source: https://www.malwarebytes.com/partners/



INTERESTED IN LEARNING MORE ABOUT HOW KONICA MINOLTA CAN HELP YOU PROTECT YOUR BUSINESS?

Workplace Hub, an all-in-one scalable system, offers a robust and reliable infrastructure, giving SMBs a level of IT security and sophistication traditionally associated with large enterprises only.

And with Sophos, world leading security provider and proud Workplace Hub partner, focused on simplifying IT for small to medium sized businesses, you get the latest software ensuring your systems are constantly monitored, protected and managed against malicious attacks and other security threats. It means your infrastructure, employees and data are always safe and secure, no matter where you work.

Find out more at workplacehub.konicaminolta.eu

workplacehub