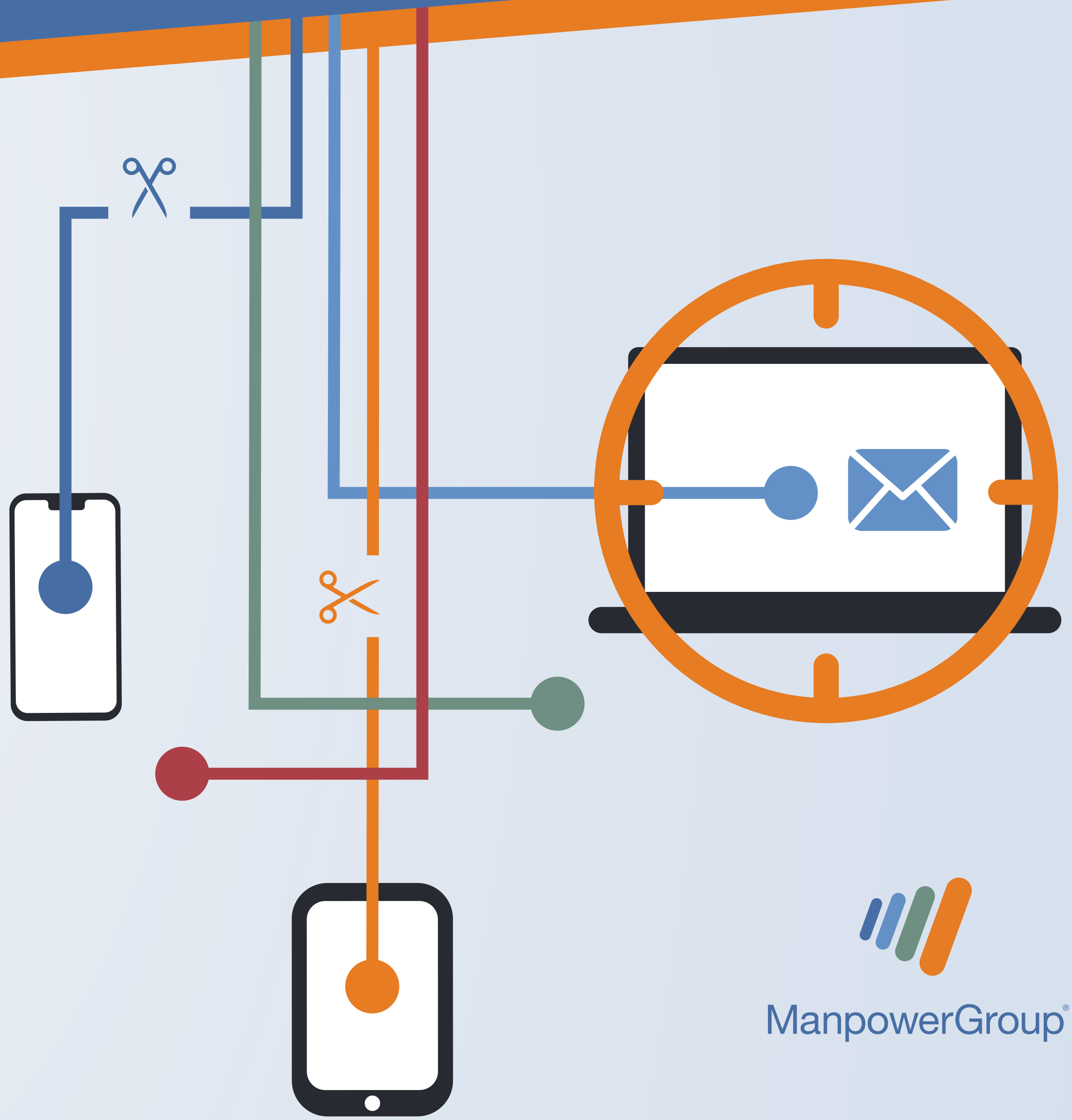
CYBER SAFE AT HOME



ManpowerGroup®

REMOTE WORKING BRINGS NEW OPPORTUNITIES – AND NEW CHALLENGES

1 **Switch off Alexa and Google Home where you're working.** Be careful when discussing confidential information if you use a smart home device - they may be listening and recording conversations. Keep devices off while working and update device privacy settings to allow you to easily delete conversations.

2 **Master the tech you use - not muting yourself is the new hitting reply all.** If video conferencing is new to you, give it a test with a colleague before going live with others. There are lots of bite-sized trainings available on Microsoft's YouTube page to get you on the fast-track to becoming an expert.

3 **Poor connection? Turn the cameras off.** Video conferencing is a great tool but can overload the network easily so consider having the camera feature on at the start of a meeting, and then switching to audio only to preserve bandwidth and improve the quality of your connection.

4 **Get creative with meeting start times.** Avoid scheduling all your meetings on the hour to preserve bandwidth – consider moving your team check in to start at 9:05 instead of 9:00.

5 **Use the collaboration tools that are authorized and supported by your company. They are safe, others may not be.** Cyber criminals have been successful in hacking several platforms that don't have end to end encryption, and some tools may even share your personal data to third parties without informing you.

6 **If you participate in a conference call that is organized by someone outside your company, ask the meeting host to confirm that privacy settings have been enforced.** This includes:
Ensure that a per-meeting ID, exclusive for that meeting, is used.
Enable "Waiting Room" features so that the moderator can see who is attempting to join the meeting before allowing them access.
Disable options such as "join before host," "screen-sharing for non-hosts" and "remote control functionality"
Lock the meeting to outsiders / uninvited guests.

7 **Be conscious of your environment and maintain client confidentiality.** If you have confidential materials around you, keep them stored in a locked drawer.

STAY ALERT FOR PHISHING SCAMS FROM TRUSTWORTHY SOURCES, ESPECIALLY NOW

One of the fastest shifts we have seen in recent weeks and months across the world is the mass movement to remote working. While we can celebrate the speed with which we and our clients could make this happen, we need to exercise even greater vigilance and caution too. With attention on new priorities for individuals and organizations, and increased online activity, cyber criminals across the world are actively working to take advantage of the situation and you.

In the last 3 weeks alone, ManpowerGroup saw a 30% increase in phishing attempts and social engineering scams. Now more than ever it is important for you to be aware of online scams and threats – they are increasingly sophisticated and much more frequent.

What's a phishing attack and how can I avoid one?

A phishing attack is when a hacker uses a legitimate-looking email or social media post to trick you into providing confidential personal data. They are designed to look trustworthy and real – but with these tips you can stay protected and keep the scammers at bay:

- **Take a pulse check, trust your gut.** Remember that phishing attacks prey on emotions like fear, greed or curiosity. Be on the lookout for threats or urgent requests and offers for prizes or monetary refunds. You know how it goes – if it looks too good to be true, it probably is!
- **Review the context, be suspicious.** Are you being asked to share personal data – bank account info, social security number, etc? These are always red flags.
- **Check the sender, and check again.** Always use caution when you see the banner at the top of your Outlook that identifies an email as outside the ManpowerGroup domain.
- **Scan the content, be on the look out.** Are there embedded links or attachments?
  - Links aren't dangerous until you click. Make hovering a habit to see the full URL destination or use a search engine to verify the site before clicking.
  - Attachments can contain malware that can infect your device and our network. Always check the file name and extension for anything suspicious.

What do I do if I've received a suspicious-looking email?

As we transform our business and become more digital, we continue to strengthen our cyber security measures to protect our people and data. Our current security solutions – including URL rewriting and attachment scanning - block over 90% of all incoming malicious email, but legitimate websites can still be compromised and phishing sites that are only a few hours old may not be caught by our tools. So we still need you to help spot phishing attacks.

- **It's easier than ever to report a phish - use the PhishAlarm button in Outlook.** Look for it either within the message preview pane or the opened message. Click and select "Report Phish." You will receive a confirmation pop-up or email that will notify you if the email you reported is suspicious, is a training exercise, or considered safe. The reported email will be automatically forwarded to a security analyst for further review.
- **Notify your local IT team.** When in doubt, better safe than sorry! If you come across something that looks phishy – reach out to your local IT team or visit the IT service desk.

COVID-19 SECURITY PRO TIPS

✓ **Only get your medical advice from trusted sources.** At a time when we are encouraged to stay informed, Cyber criminals are posing as legitimate government or health organizations with important information (or misinformation!). Always look to the World Health Organization (WHO) and your local department of health to get the latest, most accurate health news.

✓ **Scammers may also exploit your charitable spirit** and encourage you to donate to fraudulent causes. Exercise increased caution when donating to charitable organizations, and always verify the charity or donation site first.

✓ **When online shopping at home, think twice before clicking "add to cart"** on a deal that seems too good to be to be true. It probably is. Don't buy things online that seem to be sold out everywhere else – it's likely a scam. Only buy from reliable vendors and check your bank account often for suspicious activity.

✓ **Teach 'em young – it's never too early to nurture good cyber security habits with your children!** With a house full of online users, it's a good time to talk to your family members about cyber safety. Listen to their online experiences and explain to them the important of being just as safe online as offline. If necessary, check the security and privacy settings of smart toys and use parental controls to safeguard your child's online activity.

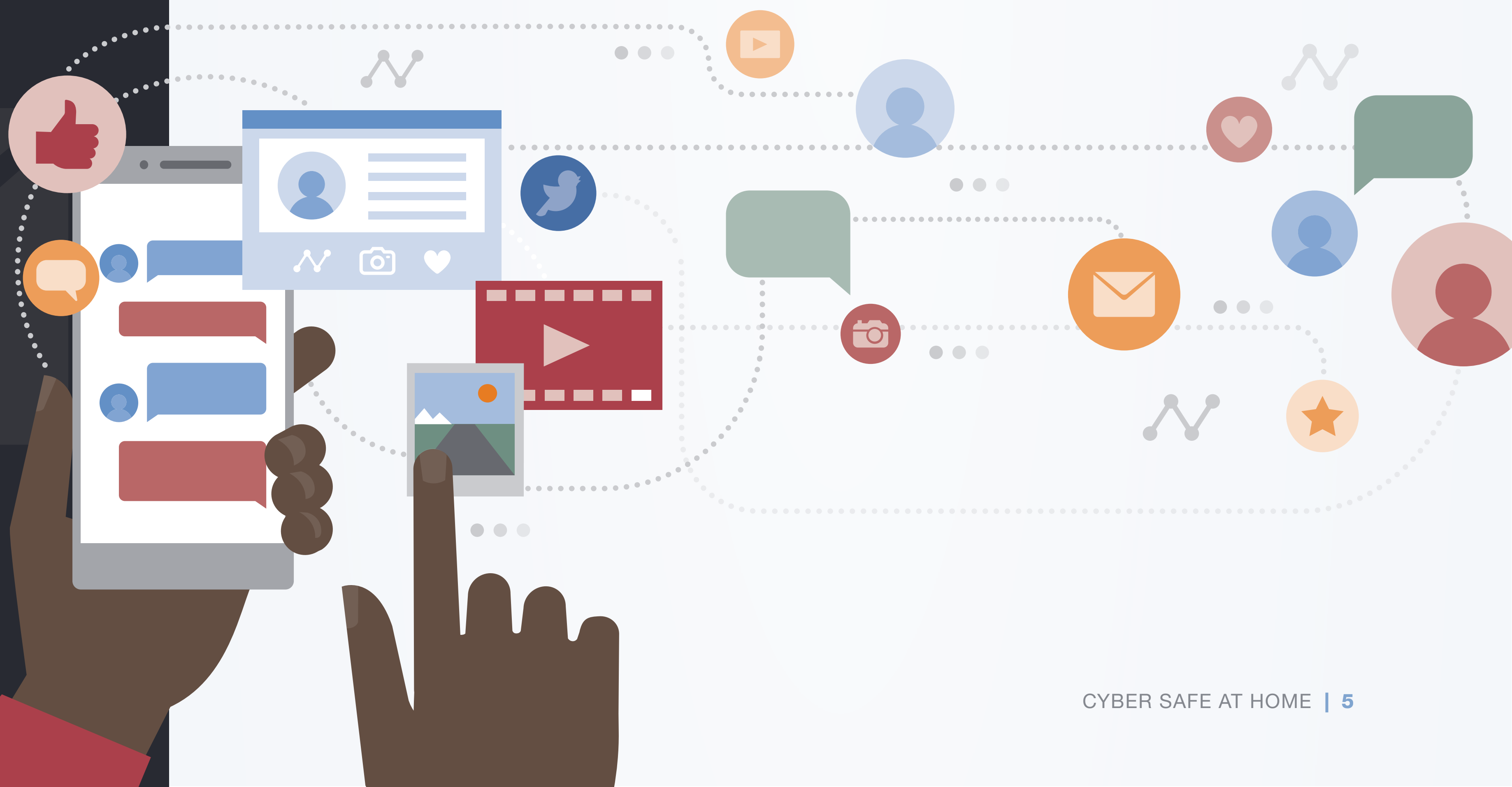
TRUSTED AND TRUE: STRONG CYBER HABITS TO KEEP NURTURING

Practice good password hygiene. Check that your internet router and other home devices are protected with a strong password or passphrase. The longer and more complex it is, the more secure it will be. **Don't get lazy with security.** Disabling privacy settings or anti-virus, using your personal email, or deploying any other "workaround" that favors availability over security is a bad idea – our network settings and tools are built to protect our data and us.

Review all your app permissions to ensure you're not inadvertently sharing sensitive information. Navigate to your privacy settings, then review – do all apps need access to your microphone AND location? Probably not. When in doubt, always choose the least amount of data-sharing.

Don't ignore the software updates. Back up your data and run software updates to ensure your devices are up to date. Privacy tools, add-ons for browsers and other patches need to be checked regularly.

Don't flood the help desk every time you encounter a problem. First, try to troubleshoot the issue on your own – ask colleagues, visit Microsoft's support site. If you still have problems, then visit the IT service desk.



As our work and home lives continue to blend, we are continuing to strengthen our cyber security practices. The good news is that the secure habits we practice while working remote will help us be protected in our personal lives too. Thanks for playing your part in keeping yourself and our data safe while working from home. If you have any questions or concerns, please reach out to your local security contact or the IT service help desk.

ManpowerGroup®