WORKING FROM HOME SECURELY

We are living in extraordinary times. The COVID-19 pandemic has rapidly changed the way we work and communicate with each other as nations swiftly roll out sweeping measures to slow the spread of the virus.

This brings new opportunities and new challenges for individuals and organisations, including working from home. As the lines between work and home are blurred, organisations must ensure their staff are working safely and are continuing to share and transmit information securely. As we face into the physical risks and put extensive measures into place, we must also consider the virtual risks associated with the COVID-19 crisis.

The increase in malicious activity against companies and individuals makes it more important than ever you and your organisation are prepared with the simple things you can do to protect your virtual valuables.

We know there is a lot to consider right now – so we have put together some tips for both organisations and individuals to help you and your staff work from home securely. We are all in this together, take care and stay safe.

LYNWEN CONNICK

Chief Information Security Officer, ANZ

CYBERSECURITY MATTERS RIGHT NOW

As organisations have activated business continuity plans to respond to this crisis, there has been a dramatic and swift increase in the number of employees working remotely. In the United States alone, it has been estimated that up to 75 million employees (over 55% of the workforce) could be working from home because of COVID-19[1]. Transitioning, on scale, to these new ways of working requires consideration for how we continue to operate with effective risk controls and keep protecting valuable data and critical systems.

With unprecedented global interest in a single topic, there is an increasing number of threat actors, both cybercriminal and state-sponsored, leveraging this pandemic. This includes a dramatic rise in fake email (phishing) and text (smishing) campaigns. These messages often impersonate official COVID-19 information providers such as government agencies or offer scarce supplies such as face masks.

The Australian Cyber Security Centre has reported an increase in COVID-19 related scams and phishing emails. They have observed thousands of newly registered websites relating to COVID-19. Some are legitimate, but many are suspected to have been created for malicious purposes[2]. ANZ Cyber Defence are monitoring COVID-19 related phishing campaigns, and are working closely with partners to ensure robust controls are in place to protect ANZ customers and systems.

Increased use of collaboration tools by remote workers, such as free cloud-based video conferencing and chat services introduce a number of risks if they are not within a company's existing controls. There is increasing concern about the access a number of these free tools provide and the level of protection provided to personal information required to establish accounts.

It's important to turn on your automatic app and software updates on all devices to ensure you have the the most recent and secure version. Using tools provided, tested, approved and monitored by your organisations is essential. It's also advised where possible to keep work and leisure separate by using a personal device for non-work related online activities.

Now, more than ever, it is critical your employees understand their responsibilities and how they can help protect your company's information, and how they can work from home securely.

ANZ takes the protection of our customers, staff and assets very seriously. We operate a global security operations centre that proactively manages our environment to ensure we adhere to strict government, privacy and regulatory requirements for information security. We are providing a range of support measures to our customers and will continue to do this throughout this challenging period.

For more information and tips on how to be safe online, please see **www.anz.com/security** or **www.anz.com/covid-19/**

1. https://globalworkplaceanalytics.com/brags/news-releases
2. https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity

MAKE A P.A.C.T.

WORKING FROM HOME SECURELY

TIPS FOR ORGANISATIONS

Working from home has become the new norm for many people, which means it's never been more important to work securely and maintain visibility over where corporate and customer information is stored and shared.

Working from home can be a great time to build capability. Your leaders are no doubt concerned about protecting information and systems in this new world. Your staff might also feel more exposed to cyber threats when working outside the office environment. Educate your team in cyber security practices, such as detecting scam messages and managing information to ensure security and privacy is maintained for both customers and your organisation. Here are some steps you could follow.

It's important to secure our workplace virtual valuables in the same way we do our physical ones.
One way to do this, is by making a P.A.C.T.

PAUSE

before sharing your personal information

STEP 1:

Ask yourself, do I really need to give my information to this website or this person? If it doesn't feel right, don't share it.

STEP 2:

Pause and consider Information Classification:
Does your organisation have an information classification approach? Do staff understand what can be shared with whom and through what channels? Talk about social media, collaboration tools etc. and decide what's right for your organisation.

Ensure staff protect and transfer information in safe ways. Remember that USBs and other forms of "removable media" can be easily misplaced or corrupted with malware by inserting them into devices that aren't secure. An option is to disable media reading or only allow media such as an encrypted USB supplied by your organisation.

ACTIVATE

two layers of security with two-factor authentication

STEP 1:

Use two-factor authentication for an extra layer of security to keep your personal information safe.

STEP 2:

Activate Multi-Factor Authentication:
Wherever possible turn on or look to implement multi-factor authentication for important tools like remote access systems and resources (including cloud services). This will provide an additional layer of security, and takes pressure off poor password management.

CALL OUT
suspicious messages

STEP 1:

Be aware of current scams. If an email, call or SMS seems unusual, check it through official contact points or report it.

STEP 2:

Call out when it's not quite right
Make sure staff know what to do if their device is lost or stolen or they experience a cyber or information security incident. It's important you can quickly respond to events and this is only possible if staff have an easy way of reporting concerns.

TURN ON
automatic software updates

STEP 1:

Set your software, operating system and apps to auto update to make sure you get the latest security features.

STEP 2:

Turn on patching
Ensure your systems, including Virtual Private Networks and firewalls, are up to date with the most recent security patches. This will ensure your systems have the latest security software on them.

CONSIDER OTHER IMPORTANT STEPS FOR PROTECTING ACCESS TO YOUR INFORMATION AND SYSTEMS:

- **Control Access:** Apply a Virtual Private Network (VPN). VPNs allow remote users to securely access your organisation's network, such as email and file services. VPNs create an encrypted network connection that authenticates the user and/or device, and encrypts data in transit between the user and your services.
- **Whitelist Software:** Ensure staff only use approved software and applications. Staff working from home may attempt to use different software to help them when away from the office environment.
- **Information Protection:** It's important to know where your information is stored and how it is shared to protect it from, and where necessary, enable a response to potential data loss or cyber compromise events.
- **Secure Devices:** Devices used for working outside an office environment are more vulnerable to theft and loss. Ensure staff understand the risks of leaving their own or their organisation's devices unattended, encourage them to keep devices somewhere safe and to lock them when they're not being used to prevent unauthorised access.

For additional controls review the **Australian Government's Signals Directorate Essential Eight** (https://www.cyber.gov.au/publications/essential-eight-explained). These represent **strategies to mitigate cyber security incidents** in a prioritised list to assist organisations in protecting their systems.

MAKE A P.A.C.T.

WORKING FROM HOME SECURELY

TIPS FOR INDIVIDUALS

Working from home means our personal space has very much become our professional space. Individuals will be handling and sharing various pieces of sensitive information at home. Therefore, it's important we bring our work practices of information handling and cyber security into our homes.

The information below sets out some basic guidance for individuals to consider when working remotely.

PAUSE

before sharing your personal information

Ask yourself, do I really need to give my information to this website or this person? If it doesn't feel right, don't share it.

WHAT DOES THIS MEAN WHEN WORKING FROM HOME?

Limit sharing: Don't send business information to your personal devices, personal email accounts or other locations not protected by your organisation. And only use approved secure file transfer tools (corporate cloud file sharing applications) or other approved mediums when sharing information.

Limit public Wi-Fi: Don't use public Wi-Fi especially when working on a company device or sharing sensitive information. Public Wi-Fi is prone to malicious attacks and cybercriminals can easily hack into these connections.

Avoid unknown links and attachments: Avoid clicking on links and attachments from unknown email senders. Especially those that are health related as scammers are exploiting people's current concerns. The scams may claim to have a 'cure' for the virus, offer a financial reward, or be encouraging you to donate. Like many scams, these emails prey on real-world concerns to try and trick people into doing the wrong thing[3].

Dispose of sensitive information securely: Don't just throw it in the trash or recycling bin. Any paperwork no longer required should be destroyed securely, especially if it contains sensitive information about cusotmers, employees or the organisation.

ACTIVATE

two layers of security with two-factor authentication

Use two-factor authentication for an extra layer of security to keep your personal information safe.

WHAT DOES THIS MEAN WHEN WORKING FROM HOME?

Make sure devices are password protected

For example, if you're using a laptop, make sure it is password-protected, locked and secure.
Never leave it unattended – like in a vehicle or at a public charging station.

3. https://www.ncsc.gov.uk/guidance/home-working

CALL OUT
suspicious messages

Be aware of current scams. If an email, call or SMS seems unusual, check it through official contact points or report it.

WHAT DOES THIS MEAN WHEN WORKING FROM HOME?

Call out incidents
Report any suspicious emails or messages via appropriate corporate channels. This enables Security Teams to protect others from similar suspicious messages at a time when we are seeing an increase in attempts to use email or malicious websites to solicit personal, often financial, information (phishing).

TURN ON
automatic software updates

Set your software, operating system and apps to auto update to make sure you get the latest security features.

WHAT DOES THIS MEAN WHEN WORKING FROM HOME?

Turn on automatic software updates
Set your software, operating system and apps to auto update to make sure you get the latest security features. Software updates often fix weaknesses in operating systems and software, including apps, which hackers use to access computers and mobile devices.

LAST BUT NOT LEAST, GO DIRECTLY TO RELIABLE SOURCES FOR NEWS AND UPDATES

Select a few credible news sources for the latest updates and type these directly into your web address bar. We have observed an increase in fake news and malicious websites attempting to compromise information and devices.

For more helpful and easy to follow tips, go to **www.staysmartonline.gov.au**

anz.com
Australia and New Zealand Banking Group Limited (ANZ) ABN 11 005 357 522. AU23318 04/2020