iOCO

Remote Work and Security **DO'S & DON'TS**

It's a brave new world for many businesses across the globe as unprecedented numbers of employees begin working remotely in the face of the Coronavirus. Here are 7 things you must know before you Work From Home

I could use a change of scenery

DON'T: Use public Wi-Fi.

DO: Make sure your network is secure, which might mean actually working from home. If you must work in a public place, utilize a VPN.

62% of Wi-Fi related security incidents occur at cafes and coffee shops [1]

DON'T: Use unauthorised personal devices for work-related tasks.

DO: Use company-issued machines. If you can, work with digital certificates to authenticate the right machines are accessing your systems.

74% of IT leaders from global enterprises report that their organisation has experienced a data breach due to a mobile security issue [2]

Let me answer that from my phone really quick

Hey guys, I found this new video messaging app online, should we give it a try?

DON'T: Download apps or new software without getting IT approval.

DO: Only utilise cloud services that have strong security policies in place (if you're not sure, ask) or that integrate with more comprehensive PKI-based security solutions.

21% of files in the cloud contain sensitive data [3]

DON'T: Share sensitive information on any platform that's not been cleared or secured by your team.

DO: Follow IT policies around internet and app usage and participate in organisation wide security training. If you can, use certificates for email encryption and authentication.

Through 2025, 90% of the organisations that fail to control public cloud use will inappropriately share sensitive data [4]

Uploading this document to the cloud is safer than email, right?

I can always go back and change my password later.

DON'T: Let your guard down.

DO: Use two or multi-factor authentication and strong passwords - always. A secure password management programme is a good way to generate and store your credentials, so you don't have to remember them off-hand.

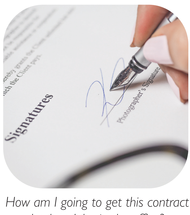
80% of hacking-related breaches involve compromised and weak credentials [5]

DON'T: Ignore anti-virus expiration notifications.

DO: Encourage your IT team to invest in centralised anti-virus management technologies designed to easily monitor and update software across the enterprise.

Everyday, at least 350,000 new malicious programmes are detected [6]

Another software update? It can wait.



How am I going to get this contract back to John in the office?

DON'T: Waste time mailing hand-signed documents between locations.

DO: Consider using digital signatures to sign time-critical contracts, policies, and other legal documents.

Businesses achieve 70% to 80% efficiency improvements after removing manual processes to adopt digital technologies like eSignature solutions. [7] **Learn more at globalsignsign.com/en/digital-signatures**

1 https://www.comparitech.com/blog/information-security/security-remote-working/
2 https://www.info.lookout.com/rs/051-ESQ-475/images/idg-report-buying-into-mobile-security.pdf
3 https://www.skyhighnetworks.com/cloud-security-blog/5-key-findings-from-2019-cloud-adoption-and-risk-report/
4 https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/
5 https://enterprise.verizon.com/resource/reports/dbir/
6 https://dataprot.net/statistics/antivirus-statistics/
7 https://www.forbes.com/forbesinsights/adobe_e-signautre/index.html

GlobalSign GMO INTERNET GROUP

Source: https://www.globalsign.com

impression™

www.impression-signatures.com