SBS INSIGHT HUB

SHARD Business Services

INTRODUCTION TO KEEPING WORK AND PERSONAL EMAILS SEPARATE - OVERVIEW

Keeping work and personal emails separate

Most people will have used their work email for something personal or forwarded a work email to a personal account so they can get work done at home. Although this may not seem much of a problem, there are many risks associated with this. It is important to keep these separate, to ensure security for both you and the organisation your work for.

Work email for personal use

Using your work email for personal use reduces your privacy. As a member of staff, your emails are not entirely private like your personal emails are, and there may be a situation in which your emails are read if your organisation has a valid legal basis to do so.

By using your work email for other things, you are risking the security of your network. If you use your work email to sign up to a shopping website, for example, and that data is part of a data breach, it increases the chance of risk. Similarly, it is possible to fall victim to various types of scams and malware, which again could lead to similar security issues. There is a much higher risk of your work account being hacked if you are using it for personal purposes.

You also risk causing a data breach by using your work emails for personal use. You are more likely to mistakenly forward or email unauthorised persons, which in turn will cause trouble for both you and the organisation.

Forwarding work emails to a personal account

It is very common for workers to forward emails to an account they have access to from home. A survey showed that 64% of workers admitted to having forwarded a work email to their personal account to catch up on work from home. Doing this can cause risk to yourself and your employer.

Research shows that 84% of people who had forwarded emails did not see anything wrong with their actions as there was no malicious intent; however, when it comes to legal judgements in cases surrounding GDPR rulings. Some reasons as to why it is important to ensure a separation of the two are as follows:

Firstly, this is a potential GDPR risk. Data subjects are not informed that their personal data will be transferred to a personal account, which breaches their rights and therefore the legislation.
It is likely that your personal systems will have different, and perhaps less effective, network security, and by forwarding personal data, the risk of breach is increased.
Similarly, using a personal device to log into work emails can also create a risk. Your personal device is more likely to be seen by unauthorised personnel, and there is no way to guarantee that any personal data included within your emails is fully protected.
In the event that you might leave your organisation, if you have avoided having personal data on a personal device or account, it ensures that you are not in breach of any data protection or confidentially rules. The ICO have acted against employees who have taken personal data with them to a new job, leaving them with a fine and a criminal record.

REMEMBER: KEEPING YOUR WORK EMAIL AND DEVICES SEPARATE FROM YOUR PERSONAL EMAIL AND DEVICES PROTECTED BOTH YOU AND YOUR ORGANISATION

shardbusinessservices.co.uk
07714651415
office@shardbusinessservices.co.uk
shardbusinessservices
shardbusiness
@shardbusiness