Reasons not to use personal email for work purposes

Free email services scan emails

Email services that allow ‘free’ mailboxes make their money from advertising. To sell adverts the contents of emails are scanned, and the results stored and used to target adverts. Therefore, emails sent to or from, or stored in, this type of account can have the contents saved and stored indefinitely. [1]

Lack of password control

As we have no control over the password the user sets on the mailbox we can’t set minimum security levels on them, making them easier to hack. They also never have to be changed, which is good practice, so once compromised will always be compromised. [2]

Saved credentials

Web mail services allow users to save their username and password on the device. Therefore if someone connects to a mailbox from a public machine and forgets to un-tick the boxes that ask about saving log-in details they may be stored. [3]

Hacked device

As we have no control over the devices used to access the email accounts we cannot say that they are patched up to date or free of malware, nor running anti-virus and firewall software.

Patching fixes known security issues with software on a device. If a patch is released and not applied, or the software is out of support and patches are not released to fix known vulnerabilities it makes the device easier to hack. [4]

Once a device is hacked someone can install malware on it. This could allow an attacker to view everything on the machine, or receive reports of keystrokes showing them what the user is typing therefore revealing confidential information to them. [5]

Hacked Web mail

Online email providers are a prime target for hackers. Users will use their personal email address to register for other sites, and may reuse passwords over multiple sites, therefore usernames and passwords for email accounts are of large value to hackers. If a large mail service provider does have a leak of account details then the emails from these accounts can be harvested. [6]

No device management if emails stored locally

Some mail providers allow email accounts to be accessed via applications installed on the device and store them in that device’s memory. We have no control over access restrictions on these devices so if someone loses that device we do not know to what standard access to the device is protected (is there an access code/password for it), the device probably won't be encrypted and there may be no way to remotely wipe data from the device. These would be the three minimum standards for allowing users to access work email accounts from a device off our premises. [7]

Mistyped address

Due to the number of accounts set up by mail providers there is more chance of a mistyped email address when sending something to yourself, or asking a college to forward something to you. E.g. if I wanted to send something to jsmith@xxxxx.com but mistyped the initial and sent it to ksmith@xxxxx.com there is every chance this is a valid address and you will never receive any message to say you go the address wrong so will never be aware of it, and even if you are aware you would have no way to know if someone else owns that address.

Also if your personal email address is similar but different to your work one there is a greater chance of confusion. If your work address is jsmith@lancaster.gov.uk but someone else has jsmith@xxxxx.com, so your personal account is jesmith@xxxxx.com, then if you ask a colleague to forward work to you they may miss your initial out as they are not used to typing it.

Finally, criminals buy up 'doppelganger' domain names for email accounts that contain similar names to large mail companies e.g. googel.com, so if you make an error after the '@' part of the address they will receive the email. .gov.uk domains are protected from this. [8]

European Union Data Protection Directive

The European Union Data Protection Directive is a legal control forbidding the transfer of data about citizens outside the EU unless certain criteria are met. Because we don't know where the emails sent to personal accounts will be stored then by sending something to a personal email address we may be in breach of this. [9]

Shared email address and device issues

A home device and email account could be used by multiple people in the household, the other users will not have read or signed up to any council policies therefore may not be as aware of the issues surrounding data protection, and they would be privy to personal information that the council needs to protect.

Known user emailing in

Because someone working from home will have the emails addresses of work colleagues stored in their address book, and those people will be used to receiving an email from that personal address. Therefore if the personal address is hacked and used to send viruses or spam all the work colleagues will receive it and be more likely to open it as it is from a trusted source, meaning we have more chance of having the core network infected. [10]

No back-up/retrieval/audit ability

Our email is backed-up so that in the event of data loss we can retrieve emails, and we can check the dates and times emails were sent and who they were sent to and from for audit purposes. Therefore if we are ever challenged over something by a supplier, contractor, member of the public etc. we have all the records we need. As soon as the email is sent to or from a personal account we lose that ability, therefore we cannot defend ourselves against claims made by third parties.

Data Protect Act and Freedom Of Information act issues

We are legally obliged to provide information when it is requested under certain acts. If all emails are processed through work systems it makes the job of retrieval relatively easy and therefore we are compliant. As soon as communications start being sent through third party software they come in scope under the acts and communications sent through them do need to be reported. However, as the council will not know they exist we find it difficult to comply with these acts and therefore will be in breach of them if we miss these communications out of the response. [11]

The Data Protection Act lists 8 principles that we must follow [12], stating the data is:

1. used fairly and lawfully
2. used for limited, specifically stated purposes
3. used in a way that is adequate, relevant and not excessive
4. accurate
5. kept for no longer than is absolutely necessary
6. handled according to people's data protection rights
7. kept safe and secure
8. not transferred outside the UK without adequate protection

By transferring the data out of our network and losing the controls we have put in place to manage data we lose control of the data and risk breaking every principle.

References

1. http://www.google.com/intl/en/policies/terms/ **Google Terms of Service** (retrieved 30.06.2015)
2. http://www.identityhawk.com/preventing-identity-theft-with-strong-passwords **The Importance of Strong Passwords in Preventing Identity Theft** (retrieved 30.06.2015)
3. https://www.surfeasy.com/blog/10-ways-to-protect-yourself-when-using-a-public-computer/?lang=0 **10 Ways to Protect Your Online Privacy When Using a Public Computer** (retrieved 30.06.2015)
4. http://www.scmagazineuk.com/patching-is-too-important-to-be-neglected/article/128089/ **Patching is too important to be neglected** (retrieved 30.06.2015)
5. http://blogs.technet.com/b/mmpc/archive/2013/04/17/everyone-benefits-from-antimalware-software.aspx **Everyone benefits from antimalware software** (retrieved 30.06.2015)
6. http://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attacks-on-popular-web-mail-services-signal-future-attacks/ **Targeted Attacks on Popular Webmail Services Signal Future Attacks** (retrieved 30.06.2015)
7. http://www.baselinemag.com/c/a/Mobile-and-Wireless/10-Best-Practices-for-Mobile-Device-Security/ **10 Best Practices for Mobile Device Security** (retrieved 30.06.2015)
8. http://www.bbc.co.uk/news/technology-14842691 **Bad spelling opens up security loophole** (retrieved 30.06.2015)
9. http://ec.europa.eu/justice/data-protection/index_en.htm **Protection of personal data** (retrieved 30.06.2015)
10. http://www.webroot.com/gb/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering **What is Social Engineering?** (retrieved 30.06.2015)
11. https://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Freedom_of_Information/Detailed_specialist_guides/official_information_held_in_private_email_accounts.ashx **Official information held in private email accounts** (retrieved 30.06.2015)
12. https://www.gov.uk/data-protection/the-data-protection-act **Data protection** (retrieved 30.06.2015)