Why does an Email address matter?

"First impressions count" is an old, somewhat superficial saying which nevertheless portrays a simple yet powerful message.

It is human nature to make snap decisions or form impressions of someone or something with minimal information but based on often subconscious factors –we instinctively "like or dislike" or we "trust or we don't trust" and these initial knee-jerk observations go deep into our mindsets.

For example, you would not deposit a family heirloom with a bank which didn't have a safety deposit box and was known to simply put such items in a room open to all.

What relevance has this instinctive judgement got to do with an email address?

When firms first start, especially sole practitioners, it is understandable that the Partner(s) setting up the firm do things in the most cost-effective (at least in the short-term) and easiest way. For most "startups" the Partners have little support and act as their own marketer, IT manager, Operations manager etc dealing with the complexity of setting up a new business with regulatory, insurance and operational challenges.

It is therefore easy to see why firms would setup an email address on a "free email platform" such as Hotmail or Gmail (*note: there are hundreds of such platforms but we will reference only the two most widely used ones*) as they are easy to setup and most of us have experience of using these accounts in our personal life.

This however, leads to three main issues:-

1) the reputational and perception risk / damage
2) an operational trap if the firm expands in terms of managing multiple mailboxes
3) lack of access to tools which law firms are expected or desire to use

For example, it is highly unlikely that you would trust a bank without an Internet presence which used Hotmail or Gmail email address. So why would clients or other professional advisers feel comfortable dealing with a law firm operating from a Hotmail or Gmail address.

These platforms enable faceless and untraceable email addresses or the preserve of the "Nigerian Prince" scam artists and untrustworthy professionals, indeed many professional firms impose restrictions on incoming emails from such platforms due to their expansive use by spammers.

There are also technical and security reasons why using these "Burner Email Addresses" is detrimental to your business and will therefore also play in the mind of other professional organisations.

It is recommended that these "free email" platforms are not used for the following reasons:-

1) **Reputational Damage**
   There is a taint of lack of professionalism associated with using a free email service for business emails. A custom domain email address (e.g., yourname@yourcompany.com) adds credibility and trust among clients and other professional partners. It demonstrates a commitment to branding and professionalism.

Where you have multiple members of staff you can employ common email addresses across your team.

It also gives the subliminal message that you are serious about security and are able to implement security tools and protection around your email domain.

2) Data Security & Confidentiality

Law firms handle highly sensitive and confidential client information. While these platforms offer basic security features, they may not meet the stringent requirements of the legal profession, particularly should your clients require you to complete a "Data or Risk Assessments" or certification such as Cyber Essentials or ISO.

Law firms need to consider the need to encrypt emails, enforce multi-factor authentication methods, and implement data protection and retention measures designed specifically for legal compliance, reducing the risk of unauthorized access and data breaches.

Furthermore, technologies such as DMARC (which can assess the true originator of emails and protect against spoofing) are becoming common and would classify these "free" platforms as high risk and potentially stop delivery of valid emails to other corporate clients or other professional advisors.

It is also not possible to configure your own "DNS" record (a record on the internet which controls your presence) so it is not possible to configure third party security tools such as email encryption, secure file send, email archiving, anti-virus scanning and the like.

Finally, as these systems are designed to provide "personal" email addresses, even if they are used for business, the data held in them is essentially owned by the people who can access them. If you have an errant employee who changes the password and refuses you access, there is probably very little you can do to get control of the account back.

3) Inadequate Email Archiving and Retention

Law firms are required to store and retrieve email communications for extended periods to comply with legal and regulatory obligations, typically requiring 7 years of email retention. The "free email" platforms fall short in meeting these specific requirements, and the ability to "route" emails to 3rd party solutions, such as Mimecast, which could provide robust archiving features, allowing law firms to securely store and easily retrieve email records and supporting e-discovery, and regulatory compliance efforts.

4) Customisation and Branding

Such platforms offer limited customisations options, which can hinder a law firm's ability to establish and maintain a consistent brand image. Custom domain email addresses and personalised email templates, available through dedicated solutions, enable law firms to reinforce their professionalism, credibility, and brand identity in every communication, fostering client trust and loyalty.

5) Collaboration

Law firms thrive on effective collaboration among teams. Whilst these platforms have basic collaboration such as shared calendars, they lack advanced functionalities commonly used in law firms such as shared inboxes, task management and integrations with practice management software.

6) Scalability and Management

As firms grow, they require email solutions which can scale seamlessly with them. If a law firm starts with one account MyFirm@Gmail.com how can it scale that when new staff arrive? Given the billions of email addresses in use on Gmail & Hotmail it is increasingly unlikely you will get the "name" you require so you would probably end up with something like

StaffName_MyFirm@Gmail.com
StaffName2_MyFirm@Gmail.com

As highlighted earlier, these will be seen as two different accounts. It will not be possible to share inboxes, task lists or calendars. As you grow, maintaining employee accounts will become burdensome.

The free platforms also have limitations on the amount of data allowed in each inbox.

7) A Scammers Paradise

Anyone can create a StaffName3_MyFirm@Gmail.com address as you have no right to the name before the @Gmail.com element of the address. Therefore by not owning your firms "domain name" you will be an easy target for cyber fraudsters who will easily be able to use your good name as a vehicle for their fraud.

Admittedly it is also possible to "spoof" a valid domain e.g. BaskervilleDrumond.com instead of BaskervilleDrummond.com but tools exist to identify such attempts, and most firms are aware of this simplistic domain spoofing. Whereas, when using a free account there is no such protection.

8) Support

The "Free Platforms" do not provide much in the form of end-user support, with most relying on "user communities" to support each other – the fact is there are so many "free accounts" in existence the vendors simply cannot provide business level support and "SLAs" are non-existent.

So what should we do?

We would highly recommend that you purchase your own domain name and a professional email hosting package. The good thing is that neither of these options are massively expensive.

1) Domain registration (.IE or .Irish) is between £10 - £20 per year depending on registration and number of years commitment.

Note: Firms who work in multiple jurisdictions often have multiple domains which all feed into the same email box. For example MyFirm.co.uk, MyFirm.Ie and MyFirm.com could all deliver email to the same mailbox.

Equally firms who have formal and "known as" names often have both domains registered. For example ReallyLongFormalLawFirmNameSolicitors.ie and Longname.ie.

2) Microsoft 365 Business Basic costs £4.90 per user per month in a package which includes:-
    a. Web and mobile versions of Microsoft 365 apps only
    b. Chat, call, meet up to 300 attendees
    c. 1 TB of cloud storage per user
    d. Business-class email
    e. Standard security
    f. Anytime phone and web support

    MS 365 licencing can be an extremely confusing model – see our article on this for more information.

    Note: Throughout this article we have raised several issues with Gmail.com email accounts, we should highlight that Google provide a business package called "G Suite" which is a competitor to MS 365 and provides Google Mail and "apps" which are similar to Word, Excel, Powerpoint and Teams but with business level support and more security than the free products. However, we find Law firms do not use this due to lack of integrations with other products and lack of familiarity with the tools.

Once you have setup the basic platform you should then consider the following elements:-

1) *What email retention is appropriate?*
2) *What backup is required over and above the vendors included backup (also linked to retention)?*
3) *What additional security tools are required?*

David Baskerville, Baskerville Drummond