THEVISIONCOUNCIL

PROPER EMAIL PRACTICES FOR CYBER SECURITY

Dan Bailey is a well-known marketing expert with numerous highly-regarded optical lab clients. Members of The Vision Council's Lab Division have access to Dan's marketing and communications consulting services tailored specifically to optical labs, and receive a discounted rate on products and services.

As an additional offering to members, Dan is writing a series of articles on topics of tremendous importance to labs. The first article of this series discussed malware and ransomware. As the main way these malicious programs are introduced into a network is through emails, we continue our discussion with email systems and why some can be preferable to others. The Vision Council encourages labs to take the precautions to avoid potentially disastrous situations, and reminds you of your access to Dan's services to protect and promote your organization.

There are four main ways to retrieve email: webmail, such as logging into your Gmail account; POP3, which uses an email client like Outlook to retrieve email from a server; IMAP, which commonly used to support multiple devices in concert with webmail services like Gmail; and Microsoft Exchange, the email manager which also works with multiple devices as well as, of course, Outlook.

In the 1990s most individual and small business emails were largely handled by webmail services from AOL, Hotmail and Yahoo. In the mid to late 2000s, most small businesses and many individuals migrated to POP3 desktop email clients, such as Outlook, because they are inexpensive to implement and typically included with website hosting packages. As time has revealed, POP3 has many shortcomings in today's real world email environment.

Most POP servers offer little or no SPAM or malware filtering, so it has been up to the individual user to install virus protection programs like McAfee or Norton. Earlier versions of webmail were not much better, and the proliferation of SPAM and Malware has especially pushed webmail providers to use their economies of scale to develop advanced detection and filtering systems. Protections provided by webmail happen automatically, which is superior to leaving the protection to the user with POP.

When Google's Gmail became a full-fledged service in 2009 it was designed to appeal to individuals and businesses alike. This move put pressure on other mail services to up their game, and now all large email players have produced superb webmail systems. These and other high-quality services, the general migration to cloud services and the ability to sync multiple devices, has resulted in a wave of people and companies returning to web-based email services rather than continuing with POP.

POP email is like an old CRT monitor compared to a new flat screen. POP still works, but it is clunky and less flexible.

There are many advantages to using either the Microsoft Online Exchange service or the Gmail service. These two services provide security, multiple device syncing, large storage capacities and data integrity. Email services - using your marketing friendly custom domain name - run about $5 per user per month for either service. In addition, both provide online storage services, communications tools such as Skype and Hangouts, and sharable calendars. Since both services keep copies of your mail in multiple data centers it is highly unlikely there will ever be a failure that loses your email, but you can keep a local copy just in case.

Whatever other varying needs you have, you need a good email system that: 1) properly represents your company, 2) is easy to use, including multi-device syncing, and 3) provides extra security through SPAM and malware filtering. If you are still on a POP email system, you should consider taking a close look at the available alternatives. At a minimal cost, the benefits in security and productivity make for a good value.

Dan Bailey | Lab Division Marketing Partner | dan@danbailey.com | 770-973-3683