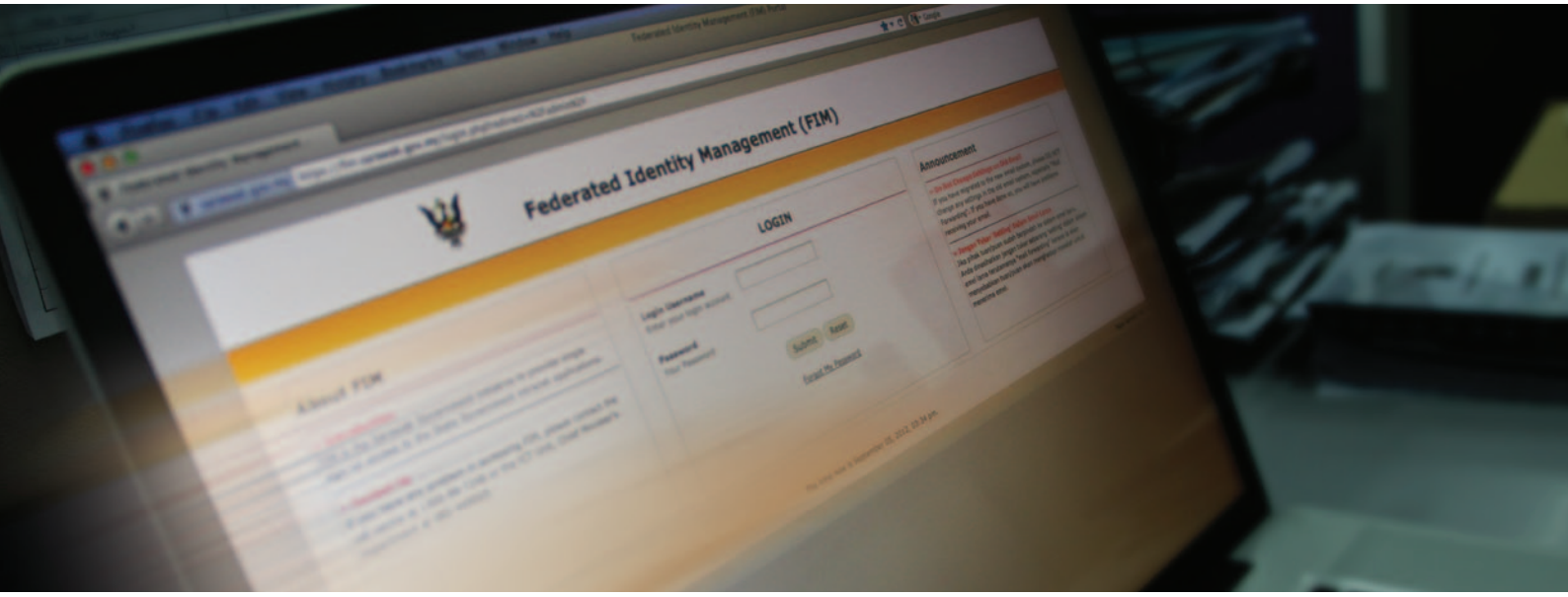
New Email Messaging System



In a move to better manage the increasing number of users and to incorporate more security features, in 2010, it was decided that the Sarawak Government would move to a new e-mail system. The move would also see the segregation of the core Sarawak Government email and addresses from other entities such as the statutory bodies and government owned companies, and a move towards a more holistic and comprehensive approach to electronic security and user policy management.

With almost 20,000 users in the system from nearly 100 agencies, the move is a huge undertaking. To take on this task there needs to be a fine level of coordination between the users, the ground support staff and the technical and implementation team. It was decided that the transition was to be carried out in several stages. This would allow the team to better manage the migration process and allow time for any unforeseen problems on the ground to be quickly dealt with.

This new email system is also the first step towards the Sarawak Government's goal of a Federated Identity Management (FIM) infrastructure platform to eventually provide users with single sign on and single identity capabilities for all government applications.

At the time of writing, the migration process is approximately 90% complete. We therefore take this opportunity to examine the progress, assess the process and reflect on lessons learnt.

Migration Process

To perform the migration, contents of the old email account are replicated to the new account as of the pre-scheduled switched over date. After a certain grace period, users are required to have fully switched over to the new email accounts and the old accounts will be removed. At that time mails from the old accounts will no longer be mirrored to the new account. To switch over, users would only need to access the FIM login page at **https://fim.sarawak.gov.my** and login using their old email account user id and password.

Even with the staggered migration, it was felt that the sains support technicians would not be able to personally attend to each of the 20,000 individual account holders; therefore an online help site was specifically created, **http://support.sarawak.gov.my**.

In addition to explaining the migration process to users, the website allows users to "Do it Yourself (DIY)" their own email accounts and provides users with the information to configure their accounts according to their needs and troubleshoot any problems they might come across.

The DIY page is divided into several sections. The first section deals with the overall interface of the webmail and "how-to" customize for general use while the second deals with configuring the email to work on desktop browser-based email clients such as Microsoft Office Outlook or Thunderbird and configuring mobile devices such as iPhone or Android phones to access the user's email server. The subsequent sections deal with topics such as configuring the calendar and address book.

A Holistic Approach to Security

FIM will allow the State Government to implement and enforce a uniform security policy across all agencies and applications used by the Sarawak Government. The single sign on and single identity feature will allow more stringent security measures to be enforced, yet at the same time allow users to more easily access applications as they need only sign in once to access the applications that they are authorized to use. FIM security measures include password strength detection where the system checks the password set by the user to determine if it is strong enough, secret questions to confirm identity, and Transaction Authorization Codes (TAC) where a one-time password is sent to the user's phone which then need to be inputted before the user can proceed. The new mail client is the first of the applications to be incorporated with FIM.

Challenges and Speed Bumps

The migration began in 2011. Because such a migration of this scale had never previously been carried out, several issues soon presented themselves. These can be divided into three categories, communication, policy and technical.

There was insufficient communication and coordination between the implementers, the support staff and the users. Although the technicians had been informed of the migration they had not been informed of the start dates for each department; due to this failure, the support technicians were caught unawares when the new system was rolled out. This lead to delays in the service response time to user queries and calls for assistance.

Another consequence of the lack of communication was that many users were unaware of the details of the migration and the existence of the self-service website, and because of this, were unable to troubleshoot their own problems.

For instance, the email service is web based, however many people were used to using a browser based system with the old system and were reluctant to switch over. How-to guides for the configuration of the mail accounts to desktop mail clients, had been put up on the DIY site so that those who wanted to continue using a desktop based system would be able to self configure their own desktop email client; however, because of the poor information sharing, many people had been unaware of that fact.

Another example is the fact that when users attempt to access the FIM some web browsers display a warning notice that the security certificate provided is not recognised. Although this is not a cause for concern, and it had been addressed in the DIY site, because information about it was not properly conveyed to the user before-hand the notice caused much confusion among the users.

In regards to policy, there were several user complaints regarding the lack of some features in the new system, for certain groups of users, which had previously been available in the old system. However, this is not caused by a defect in the new system but is the result of conformance to State Government ICT security policy.

On the technical front, a portion of users experienced the birth pangs of the new system. The implementation of any new system will always bring with it complications that were not caught during the testing stages, as even the most rigorous tests cannot compete with 20,000 dedicated users. In this case, the problems manifested as a problem within the migration script, where the old email contact addresses were not migrated. Other problems included an isolated case of user Ids being different for the old and new mails, and slow email access.

Another complaint was about the anti-spam filter. Users complained that the filter was blocking their legitimate emails and that there was no way for these mails to be retrieved. To rectify this problem the team loosened the spam thresholds of the filter. An anti-spam quarantine box was also built to allow users to retrieve any legitimate mails that registered as a false positive.

Like the email, the quarantine box can be accessed through FIM. Using the box, users can view all their emails and the classifications of the emails such as spam, high spam, infected, etc. Through the system, users can designate whether a mail is spam or not. Users can also white list an address to indicate that it is trusted so that no mails from that address are detained or black list an address so that no mails from that address get through to the users mailbox. Using the system, users can also view reports on the mails received.

The Dark Side of Spam

One of the worse days of Adam's life began with a call from his friend Ryan. Had Adam, Ryan wanted to know, sent him an email that morning?

Adam was puzzled, he hadn't contacted Ryan in at least a week. Worried he quickly checked his email. To his horror he discovered that he was unable to access it, someone had changed his password. All across the country family, friends and acquaintances were receiving what they thought were emails from Adam, and not all of them were savvy enough to give him a call to confirm the authenticity of them.

It had all begun the day before when Adam had opened an email from what appeared to be a courier company about the delivery of a package he had ordered. As he often shopped and ordered goods online, he had not thought much about it and had clicked on the link provided in the mail. The link had brought him to an innocent looking delivery company site and had brought to his computer a far from innocent virus that had hijacked not only his email but also his computer. In addition to sending out virus infected e-mails from his account the virus has also uploaded malicious content to his computer and stolen the saved passwords and information kept on his computer.

All over the world similar stories are being played out over and over again. Once only an annoying distraction, spam email has become a dangerous threat to the unwary. Although the total number of spam mails has gone down over the past few years as anti spam technology has gotten better at filtering out spam from legitimate emails, the number of malicious emails has risen alarmingly. And these emails are much more difficult to detect than the spam mail of old which sent out its message in bulk and invited you to sample the latest in 'performance' enhancing pills.

This new breed of spam mail is far sneakier that its old school counter part. I'm sure we all know not to trust emails from Nigerian princes, and we are usually wary of people who purport to offer large sums of cash as part of a contest we do not quite remember entering, but would we exhibit the same wariness when the email comes from our bank requesting that we update our information, or a courier company with a message about the book that was ordered online last week or even a friend who wants to recommend an interesting site?

This form of spam, called phishing, attempts to draw in the unwary by posing as emails from legitimate sources. Some spammers are even able to obtain information such as a bank's customers to tailor their attacks to the victim; hence makes this type of spam much more difficult for anti spam software to detect and stop. And once the mail gets through the anti spam system they could trick incautious individuals into opening them just as Adam did.

These mails might attempt to get a person to give away their usernames and passwords or they might contain links to fake sites that will upload viruses to your computer. The viruses could then steal the passwords saved on your computer or open up back doors in your computer to allow in hackers.

Keeping Safe

These days practicing vigilance is more important than ever. It is no longer enough to keep away from the seedy underbelly of the Internet to avoid viruses and hackers as now they come knocking on your door. To keep your email safe you should keep in mind some simple rules.

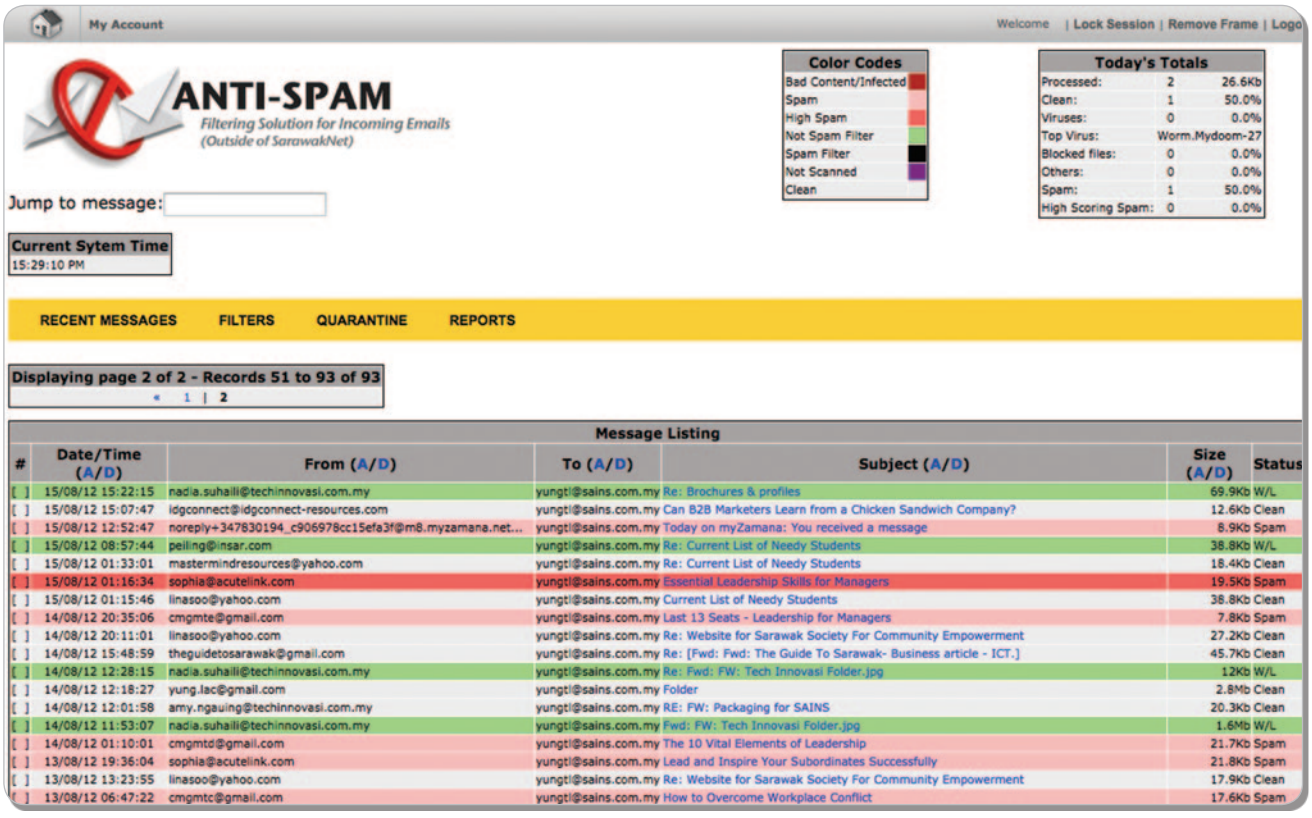
Ensure your email service is secure with adequate protections, anti spam and virus scanners. The new Sarawak Government email has upgraded its security and is now more secure that ever with beefed up email protocols and more stringent password controls. Every email is automatically scanned for viruses before being allowed into the users inbox and a TAC is needed to reset passwords.

Never give out personal information over email, even to what looks like a reliable source. Instead, go to the actual website to check if the email is legitimate. As a corollary, be wary when presented with a link to a website in an email as scammer can and do create near identical sites to websites of official entities such as banks to trick the unwary.

Opt for tighter spam control rather than looser. It is better to have false positives where a legitimate email is stopped rather than let a dangerous mail through. The spam detection system of the Sarawaknet email allows users to check for emails that have been blocked with its two-part spam filter system. The system first filters and stops the spam it detects from getting into the user's inbox. The filtered emails are then placed in a separate quarantine box which users can access to manage the blocked mails. At the quarantine box, users can release legitimate mails as well as block spam. The system also allows users to white list or black list email addresses. This ensures that emails from trusted sources will always get through while emails from spammers are blocked.

If you do receive an email from a trusted source such as a friend that you are unsure about, give that friend a call rather than giving the mail the benefit of the doubt as impersonating a person through email is as simple as knowing their name.

Don't opt to save important passwords on your computer. That way, if, in spite of everything, your security is compromised the damage will be lessened.



Screen of FIM Anti-Spam Filtering Report