Sophisticated Spam Attack

By Dan McGarry

A SOPHISTICATED FAKE EMAIL message was sent to a number of Government of Vanuatu email addresses within the last week, according to a warning circulated from the Office of the Government Chief Information Officer, or OGCIO.

OGCIO is responsible for government-wide ICT systems and services, including computer security.

The email bears a striking resemblance to an earlier notice circulated by the OGCIO help desk, announcing an upgrade of the Government email system. The malicious email, however, reveals itself in its details. The FROM: field contains an address that is not in the .gov.vu domain, and the TO: field is a GMail address.

The main difference, however, is that a line has been inserted, telling the user to complete their transition to the new system by clicking on a link. This link points to a free web-hosting provider known as wix.com. This hosting service is commonly used to run software exploits because it allows users to set up a website free of charge.

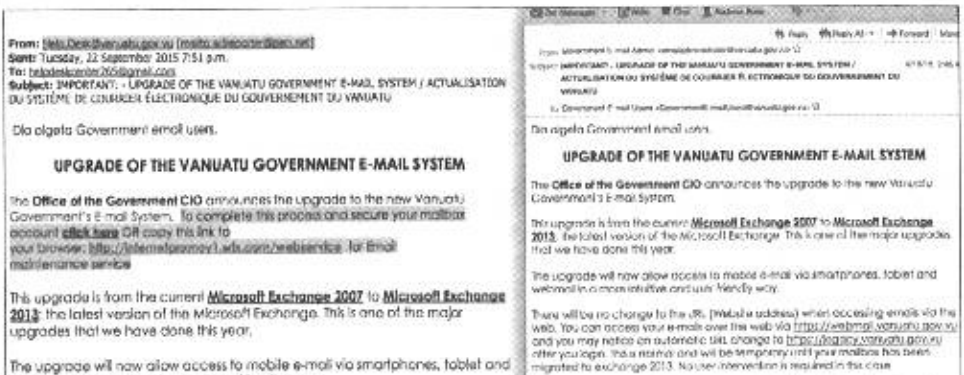
The Daily Post visited the wix.com address and found that the malicious website had already been taken down.

Email users are reminded to take several basic precautions before responding to messages:

- Verify the TO: and FROM: addresses. If the actual email address is not visible, place your mouse pointer over the address, and wait for the address to be revealed.
- NEVER click links on a security-related email unless you specifically requested the change.
- Hover your mouse pointer over links before you click them. If the address in the tooltip is not the same as the one printed, do not click on it. Report it to your IT administrator.

Electronic scams and malicious software infections are common on the internet. They take a number of common forms:

Story continues on page 5



From: [illegible]
Sent: Tuesday, 22 September 2015 7:51 p.m.
To: [illegible]
Subject: IMPORTANT: - UPGRADE OF THE VANUATU GOVERNMENT E-MAIL SYSTEM / ACTUALISATION DU SYSTÈME DE COURRIER ÉLECTRONIQUE DU GOUVERNEMENT DU VANUATU

Dia olgeta Government email users.

UPGRADE OF THE VANUATU GOVERNMENT E-MAIL SYSTEM

The **Office of the Government CIO** announces the upgrade to the new Vanuatu Government's E-mail System. To complete this process and secure your mailbox account **click here** OR copy this link to your browser: http://internetgoonev1.wix.com/webservice for Email maintenance service

This upgrade is from the current **Microsoft Exchange 2007** to **Microsoft Exchange 2013**; the latest version of the Microsoft Exchange. This is one of the major upgrades that we have done this year.

The upgrade will now allow access to mobile e-mail via smartphones, tablet and webmail in a more intuitive and user friendly way.

There will be no change to the URL (Website address) when accessing emails via the web. You can access your e-mails over the web via https://webmail.vanuatu.gov.vu and you may notice an automatic URL change to:https://legacy.vanuatu.gov.vu after you login. This is normal and will be temporary until your mailbox has been migrated to exchange 2013. No user intervention is required in this case.

Having said the above, OGCIO will allow a period for transition between the old interface and the new interface. This means that users may be prompted for

Dia olgeta Government email users.

UPGRADE OF THE VANUATU GOVERNMENT E-MAIL SYSTEM

The **Office of the Government CIO** announces the upgrade to the new Vanuatu Government's E-mail System.

This upgrade is from the current **Microsoft Exchange 2007** to **Microsoft Exchange 2013**; the latest version of the Microsoft Exchange. This is one of the major upgrades that we have done this year.

The upgrade will now allow access to mobile e-mail via smartphones, tablet and webmail in a more intuitive and user friendly way.

There will be no change to the URL (Website address) when accessing emails via the web. You can access your e-mails over the web via https://webmail.vanuatu.gov.vu and you may notice an automatic URL change to https://legacy.vanuatu.gov.vu after you login. This is normal and will be temporary until your mailbox has been migrated to exchange 2013. No user intervention is required in this case.

Having said the above, OGCIO will allow a period for transition between the old interface and the new interface. This means that users may be prompted for double login until your mailbox has been migrated then you will only be prompted to login once. And if you notice malfunction with your Microsoft Outlook, close it and open again. This would mean that your mailbox was migrated while your Outlook was open. Please refer to the user manual.

However, no configuration changes have been anticipated for Microsoft Outlook 2007, 2010 or 2013 and users will continue to access their e-mails as normal.

The only major change is the Outlook Web App interface however if you are already using Microsoft Outlook 2013 then the interface is similar. The new user interface has a more look and feel feature.

The malicious email (left) contrasted with the legitimate version (right). The altered sections are highlighted.

Sophisticated Spam Attack

From Page 3

So-called 419 scams (sometimes called Nigerian Prince scams): These consist of a person asking for assistance in transferring a large sum of money. They claim to need enough money to pay the transfer fees before the money can be sent. The victim sends the money, and never hears from the scammer again.

Lottery scams: Similar to the 419 scam, this consists of a notice that the recipient has won a lottery prize, and that they need only to pay an administrative fee before the prize money is transferred to them. The recent P&O bogus employment emails are a variation on this scam.

'Phishing' scams: The email circulated to Government of Vanuatu staff is a so-called 'phishing' scam. It consists of a near-perfect facsimile of a legitimate email, used to entice the user into clicking a link that leads to malicious software. This software is often used for identity theft, logging keystrokes to steal passwords, bank account information and the like.

It is possible that the email in question would have been used in an attempt to access Government bank accounts and resources.

Virus and trojan horse scams: An email with an attachment containing malicious software is sent, and the recipient is enticed to open it using a number of tactics. Commonly, the malicious attachment masquerades as a naughty or scandalous picture. In some cases, the attachment is aimed specifically at one person, and the attachment is made to look like a file the person was expecting.

The latter tactic was used as the first step in an attack on Google's infrastructure in China a few years ago.

As a rule of thumb, email users are reminded that if a message sounds too good to be true, it almost certainly is. Also, security verification notices (such as unscheduled password updates and the like) are never sent by email, precisely to avoid this kind of situation.