Spam, Malware, Phishing how to report and distinguish

Spam, Malware, Phishing

This page is a short overview of what communication you process you may follow when your device has been identified as a source of SPAM or possible infringement.

REPORTING SPAM, MALWARE AND PHISHING

At Stellenbosch University, we encourage our customers to submit potential spam, malware and phishing examples for review. Using these submissions, the CSIRT team can learn from the analysis of these messages. This collectively helps to improve the level of virus and spam detection.

SUBMITTING EXAMPLES

Spam or phishing examples must be sent in either.EML or .MSG format as an attachment and must not be forwarded. This ensures the original email can be analysed with its full Internet message headers intact.

The best way to manually submit an example is to:

1. Create a new message.
2. Drag and drop the email into the new message, so it is added as an attachment.
3. Send to csirt@sun.ac.za

Alternatively, use the mail application to save the email (usually located under File | Save As) as an .EML or .MSG format to a folder location, and attach the saved file to a new email.

Basic Service desk process for handling SPAM service requests

OFFICE 365 VERIFICATION" PHISHING SCAM FROM COMPROMISED STUDENT ACCOUNT

Please be on the lookout for the following phishing scam coming this morning from a compromised student account:

The subject will be "Office365 E-mail Verification" (or a variation) and says that "you recently made a request to terminate your Office365 mail" and to click on a link to cancel this termination.

The mail should be immediately suspicious to most people with common sense and awareness of phishing scams, but here are a few signs:

1. Why is a **student account** sending you mail about your "termination" of an Office365 account?
2. Why are they **threatening** you to verify or lose your account?
3. Why does the **link point to a site that is not in the university network** and is in Brazil of all places?
4. Why is something as "important" as this being **sent in a non-secure email?**

Here is an example of one of these phishing emails that several observant students and colleague have sent me this morning already!

blocked URL

If you have accidentally clicked on the link and given your login details to the phishers it is vitally important that you immediately go to the USERADM page (either http://www.sun.ac.za/password or www.sun.ac.za/useradm and change your password immediately. *(Make sure the new password is completely different and is a strong password that will not be easily guessed, as well as changing the passwords on your social media and private e-mail accounts, especially if you use the same passwords on these accounts.)*

This page covers all your spam, malware, email phishing related documentation

Find current articles on spam related issues listed here: