COMPUTER SECURITY BULLETIN

Risk/Impact Rating: SERIOUS

< Phishing Attempt Threat Advisory: “Mailbox Quota Exceeded” >

Description:

Phishing is a fraudulent process used by spammers to acquire sensitive information from users such as usernames, passwords, and credit card details.

It can also involve sending malicious attachments or website links in an effort to infect computers or mobile devices.

Phishing scam:

- Wrong spelling and bad grammar;
- Suspicious links in email;
- Threats; and
- Spoofing popular websites or companies.

In recent days, GovMail Support learned a new phishing attack that attempts to draw the attention of recipients with the subject line “ **Mailbox Quota Exceeded**”, while the sender may appear to be "**Farmácia Boa Vista 2 <farmaciabv2@sms.curitiba.pr.gov.br>**". Users are directed to a fake website and asked to enter private information. In that event, immediately close the message and report it as spam.

GovMail traffic is filtered by their anti-spam and antivirus service, which provides you with protection against dangerous viruses and spam. However, some spam may occasionally get through to your inbox or be diverted to your Junk folder, so please be cautious.

Recommendations / Solutions / How To's:

For PNP Personnel

- Use hard and different password in every site you visit. Random letters and numbers. Change them frequently;
- Verify any emails sent from a friend or banks and businesses;
- Use your spam filter if you detect a phishing email, mark the message as spam and delete it;
- Never respond to a message from an unknown source; and
- Never click any embedded links.

For Key officers and Technical Staff

- Train users to recognize, avoid and report suspicious emails;
- Implement, maintain and update security technology and processes; and
- Investing in actively updated threat intelligence and expertise.

References:

Phishing Attempt Threat Advisory: "Mailbox Quota Exceeded" (GovMail Support)

http://searchsecurity.techtarget.com/definition/phishing

http://www.actionfraud.police.uk/fraud-az-phishing

https://www.microsoft.com/en-us/safety/online-privacy/phishing-symptoms.aspx