CMSGu2018-01

National Computer Board

Mauritian Computer Emergency Response Team
Enhancing Cyber Security in Mauritius

Best Practice Guide on Handling Unsolicited E-mails

CERT-MU

National Computer Board
Mauritius

Version 1.0

January 2018

Issue No. 1

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

Table of Contents

What are unsolicited e-mails?

Unsolicited e-mails are unwanted messages that have not been requested from a company or an individual or of which the receiver is not a customer. These e-mails are also commonly referred to as spam.

Spam can come from various organizations, companies or can even contain links to phishing websites or computer viruses. Companies or individuals can get your e-mail address from the web. Other sources exist such as marketing lists that you sign up to and are passed between companies.

What to do if you receive spam?

- E-mail headers may be forged for the majority of spam. So, you should not reply to spam e-mails as it can result in you spreading spam in turn.
- You should delete spam e-mails straight away or move them to your junk folder.
- You should not click on any links provided in spam e-mails as the links may redirect you to phishing websites or malicious content.
- You should not reply to an e-mail address to unsubscribe from a list unless the address is from a recognized organization. These unsubscribe e-mail addresses may also be fake or may be used to confirm that the spam e-mails were originally sent to a valid and active e-mail account.
- You should not respond to a website that allegedly allows you to remove yourself from the list. This is because once you access the website your details are logged. You could also be exposed to illegal content or pornography.

How can you reduce the amount of spam that you receive?

- **Use an e-mail filter**

  Check your e-mail account to see if it provides a tool to filter out potential spam or to channel spam into a bulk e-mail folder. You might want to consider these options when you are choosing which Internet Service Provider (ISP) or e-mail service to use.

- **Limit your exposure**

  Use two e-mail addresses, one for personal messages and one for shopping, newsletters, chat rooms, coupons and other services. Consider using a temporary e-mail address service that forwards messages to your permanent account. If the temporary address begins to receive spam, you can deactivate it and create a new one, without affecting your permanent address.

  Moreover, do not display your e-mail address in public. This includes on blog posts, in chat rooms, on social networking sites, or in online membership directories. Spammers use the web to harvest e-mail addresses.

- **Check privacy policies and uncheck boxes**

  Check the privacy policy before you submit your e-mail address to a website. See if it allows the company to sell your e-mail to others. Do not submit your e-mail address to websites that will not protect it.

  When submitting your e-mail address to a website, look for pre-checked boxes that sign you up for e-mail updates from the company and its partners. Some websites allow you to opt out of receiving these mass e-mails.

- **Choose a unique e-mail address**

  Your choice of e-mail addresses may affect the amount of spam you receive. Spammers send out millions of messages to probable name combinations at large ISPs and e-mail services, hoping to find a valid address. Thus, a common username such as “sarah” may get more spam than a more unique name like “5arah5789”.

How can you help reduce spam for everyone?

Do not let spammers use your computer. You can help reduce the chances that your computer will become part of a botnet by:

- **Using good computer security practices**
  Disconnect from the internet when you are away from your computer**.** Hackers cannot access your computer when it is not connected to the internet.

- **Being cautious about opening any attachments or downloading files from e-mails you receive**
  Do not open an e-mail attachment, even if it looks like it is from a friend or coworker unless you are expecting it or you know what it is. If you send an e-mail with an attached file, include a message explaining what it is.

- **Downloading free software only from sites you know and trust**
  It can be appealing to download free software such as games, file-sharing programs, and customized toolbars. Bear in mind that free software programs may contain malware.

How can you report spam?

Forward spam e-mails to:

- **Your email provider**

  At the top of the message, state that you are complaining about spam. Some e-mail services have buttons that allow you to mark messages as junk mail or report them as spam.

- **The sender's e-mail provider, if you know are able to determine out who it is**

  Most web mail providers and ISPs want to remove spammers who abuse their system. Again, make sure to include the entire e-mail and mention that you are complaining about spam.