# MESSAGE FORM

(INSTRUCTION: FILL-UP BOXES INSIDE DOUBLE LINES ONLY)

*FOR COMCEN/SIG USE*

PRECEDENCE ACTION/PRECEDENCE INFO
**"PRIORITY"**

**FM: CG, PA**

**TO: All Unit Commanders**
**Attn: G6/Signal Officer/IS Officer**

**INTERNAL: All G-Staff, Personal, Special & Tech Staff, C, AOC/SAGS/XA**

**INFO: CSAFP**
**Attn: J6**

GROUP:
**24 February 2016**

SECURITY CLASSIFICATION:
**CONFIDENTIAL**

ORIGINATOR:
**6/CMB 2402-45-2016**

1. References:

   a. Command Guidance, and;
   b. VAPT and PANET Monitoring Result.

2. As per above references, forwarded is the Cybersecurity Bulletin Number 048 with topic regarding **Using Caution with Email Attachments.**

3. ITR, all concerned G6/Signal Officers/Information System Officer/NCOs are reminded to include this information as part of TI & E on all of its subordinate units as part of enhancing the Cybersecurity Awareness of the Philippine Army.

4. For information and widest dissemination.

| **DRAFTER'S NAME AND TITLE** | **PHONE NR:** |
|---|---|
| LTC JOEY T FONTIVEROS (INF) PA<br>Chief, CMB, OG6, PA | 6630 |
| **RreleaseR'S NAME AND TITLE** | |
| COL VENER ODILON D MARIANO GSC (SC) PA<br>AC OF S FOR CEIS, G6, PA | |

HEADQUARTERS
PHILIPPINE ARMY
***OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS, G6***
Fort Andres Bonifacio, Metro Manila

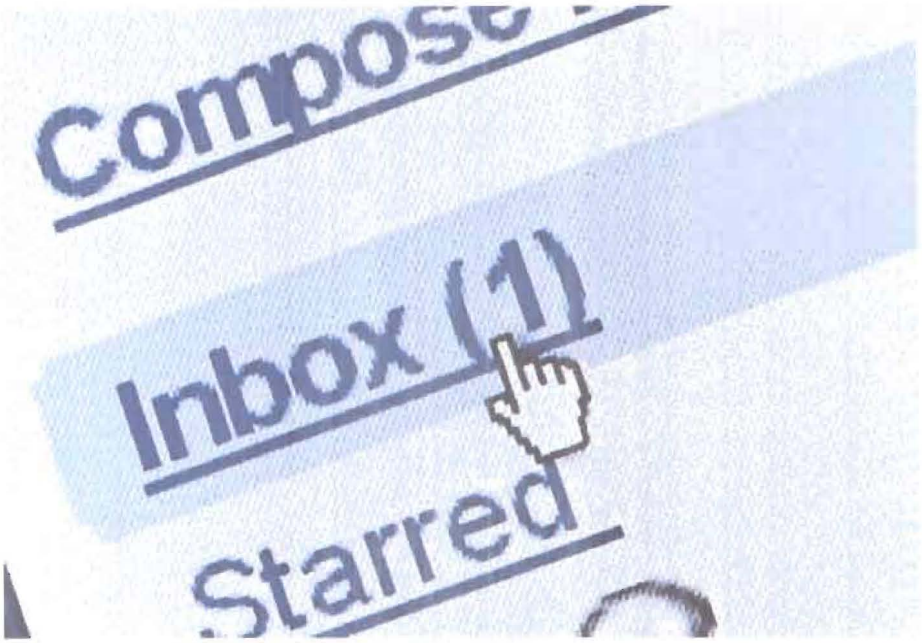
6/CMB

23 February 2016

**CYBERSECURITY BULLETIN**

**Cybersecurity Bulletin: #48**

**Using Caution with Email Attachments**

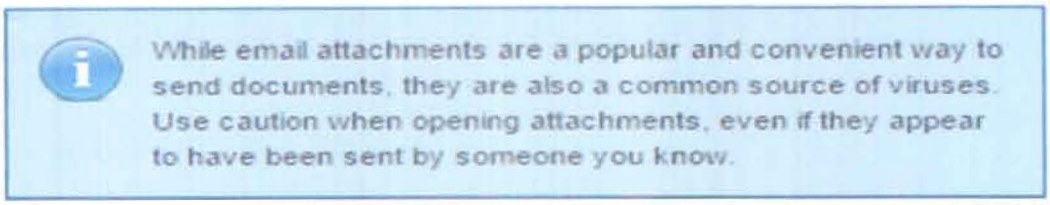



**Why can email attachments be dangerous?**

Some of the characteristics that make email attachments convenient and popular are also the ones that make them a common tool for attackers:

- **Email is easily circulated** - Forwarding email is so simple that viruses can quickly infect many machines. Most viruses don't even require users to forward the email-they scan users' computer for email addresses and automatically send the infected message to all of the addresses they find. Attackers take advantage of the reality that most users will automatically trust and open any message that comes from someone they know.

- **Email programs try to address all users' needs** - Almost any type of file can be attached to an email message, so attackers have more freedom with the types of viruses they can send.




- **Email programs offer many "user-friendly" features** - Some email programs have the option to automatically download email attachments, which immediately exposes your computer to any viruses within the attachments.

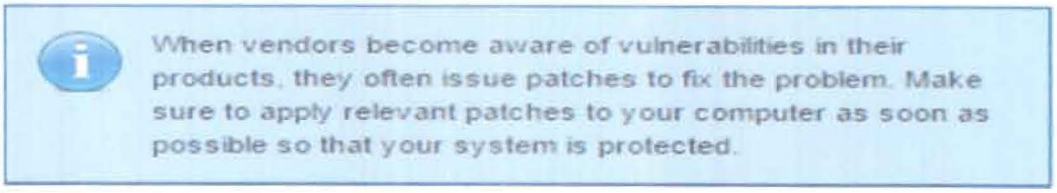
**What steps can you take to protect yourself and others in your address book?**

- **Be wary of unsolicited attachments, even from people you know** - Just because an email message looks like it came from your mom, grandma, or boss doesn't mean that it did. Many viruses can **"spoof"** the return address, making it look like the message came from someone else. If you can, check with the person who supposedly sent the message to make sure it's legitimate before opening any attachments. This includes email messages that appear to be from your ISP or software vendor and claim to include patches or anti-virus software. ISPs and software vendors do not send patches or software in email.

- **Keep software up to date** - Install software patches so that attackers can't take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.

**What are patches?**

Similar to the way fabric patches are used to repair holes in clothing, software patches repair holes in software programs. Patches are updates that fix a particular problem or vulnerability within a program. Sometimes, instead of just releasing a patch, vendors will release an upgraded version of their software, although they may refer to the upgrade as a patch.




**How do you find out what patches you need to install?**

When patches are available, vendors usually put them on their websites for users to download. It is important to install a patch as soon as possible to protect your computer from attackers who would take advantage of the vulnerability. Attackers may target vulnerabilities for months or even years after patches are available. Some software will automatically check for updates, and many vendors offer users the option to receive automatic notification of updates through a mailing list. If these automatic options are

available, we recommend that you take advantage of them. If they are not available, check your vendors' websites periodically for updates.

Make sure that you only download software or patches from websites that you trust. Do not trust a link in an email message- attackers have used email messages to direct users to malicious websites where users install viruses disguised as patches. Also, beware of email messages that claim that they have attached the patch to the message-these attachments are often viruses.

- **Trust your instincts** - If an email or email attachment seems suspicious, don't open it, even if your anti-virus software indicates that the message is clean. Attackers are constantly releasing new viruses, and the anti-virus software might not have the signature. At the very least, contact the person who supposedly sent the message to make sure it's legitimate before you open the attachment. However, especially in the case of forwards, even messages sent by a legitimate sender might contain a virus. If something about the email or the attachment makes you uncomfortable, there may be a good reason. Don't let your curiosity put your computer at risk.

- **Save and scan any attachments before opening them** - If you have to open an attachment before you can verify the source, take the following steps:

1. Be sure the signatures in your anti-virus software are up to date
2. Save the file to your computer or a disk and scan it with virustotal.com.
3. Manually scan the file using your anti-virus software.
4. If the file is clean and doesn't seem suspicious, go ahead and open it.

- **Turn off the option to automatically download attachments** - To simplify the process of reading email, many email programs offer the feature to automatically download attachments. Check your settings to see if your software offers the option, and make sure to disable it.

- **Consider creating separate accounts on your computer** - Most operating systems give you the option of creating multiple user accounts with different privileges. Consider reading your email on an account with restricted privileges. Some viruses need "administrator" privileges to infect a computer.

- **Apply additional security practices** - You may be able to filter certain types of attachments through your email software or a firewall.

**This was cross posted from:**
https://www.us-cert.gov/ncas/tips/ST04-010

https://www.us-cert.gov/ncas/tips/ST04-006

**DO YOU WANT TO KNOW MORE? TALK TO US.**

**POCs:**

a. **LTC JOEY T FONTIVEROS (INF) PA** – Chief, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0917-628-1057. Email: fontiverosjt@army.mil.ph.

b. **Sgt Mark Dave M Tacadena (SC) PA** – Branch NCO, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0998-534-2877. Email: tacadenamdm@army.mil.ph.