# 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:
**03 February 2017**

SECURITY CLASSIFICATION:
**CONFIDENTIAL**

ORIGINATOR:
**6/CMB 0302-88-2017**

1. References:

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

2. As per above references, forwarded is the Cybersecurity Bulletin Number **17-05** with topic regarding **Data Breach - The Best Defense is Vigilance**.

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 (SC) PA<br>Chief, CMB, OG6, PA | 6630 |
| **RELEASER'S NAME AND TITLE** | |
| COL VENER ODILON D MARIANO GSC (SC) PA<br>AC of S for C4S, G6, PA | |

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

6/CMB 03 February 2017

**CYBERSECURITY BULLETIN**

**Cybersecurity Bulletin: #17-05**

**Data Breach - The Best Defense is Vigilance**

There have been several high-profile data breaches impacting millions of consumers in the past year. And along with the details come the constant reminder to be vigilant. Consumer security expert Gerry Egan says awareness is key, but so is understanding what the thieves are after, so you can make it harder for them to win.

Egan answers some commonly asked questions about shopping and credit card safety:

***So what is being stolen and how is it being used?***

In point of sale (POS) breaches, thieves are stealing your 16-digit credit card numbers. Those numbers are most useful to thieves (and most harmful to you) in the geographical area near where you live. They can take those numbers, attach them to magnetic strips on different cards, and use them in brick & mortar stores. As long as

those stores are located in zip codes where you usually shop, the transaction won't raise any red flags.

It's more difficult for stolen credit card information to be used online, because most retailers have authentication procedures that require expiration dates, billing zip codes and card verification values (CVV). Still, fraudulent online purchases are possible. So keep tabs on your monthly card statements, because the threats are still out there.

***If my credit card information is stolen, is my identity next?***

Identity thieves need your date of birth, social security number and other information before they can launch significant fraud. That's not information typically shared during a POS transaction. The missing pieces of your identity won't be there to go on a rampage under your name.

***What can I do to stay safe?***

Stay alert. The law is on your side, so use your protection. Anti-fraud laws protect you from being responsible for purchases you didn't make. Ultimately, credit card companies want your business, so they will also work with you to track fraudulent purchases. All you have to do is stay alert. Check your credit card statement every month. It's common for thieves to hold on to stolen credit card numbers. That means it could be months before they actually make a purchase. Reporting strange or fraudulent activity as soon as you notice it helps banks help you get your money back.

***Should I just use my debit card?***

You can use any payment method you want. The risk adjusts accordingly. Obviously carrying large amounts of cash comes with one set of risks. The same can be said for debit cards. The numbers attached to the magnetic strip on your debit card work the same as those attached to your credit cards. If those numbers are stolen, thieves can make the same fraudulent purchases. The only difference is that the money will come from your personal checking or savings account. That's money you won't be able to use for rent, mortgage, tuition or other bill payments.

**Remember**

Credit card data breaches are viruses that attack the POS terminals in stores. While stores do encrypt and transfer that data, there remain small opportunities for thieves to get your information. Businesses and credit card companies are constantly working to mitigate these risks, but change takes time.

"Be aware," says Egan. "Live your life, but be aware. If you see something unusual, call your bank."

**Reference:**

**This was cross posted from:**

https://community.norton.com/en/blogs/norton-protection-blog/data-breach-best-defense-vigilance

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

**POCs:**

a. **LTC JOEY T FONTIVEROS (SC) PA** – Chief, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0917-6281057. Email: fontiverosjt@army.mil.ph.

b. **MAJ MAJ GIL P TARIO II (SC) PA** – Assistant Chief, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0917-7982005. Email: tariogp@army.mil.ph.