



WWW.MARFORRES.MARINES.MIL

MARINEFORCESRESERVE | APRIL 2016

# COMMUNICATOR

## BY THE NUMBERS

\* As of March 15, 2016



**LT. GEN. REX C. MCMILLIAN**

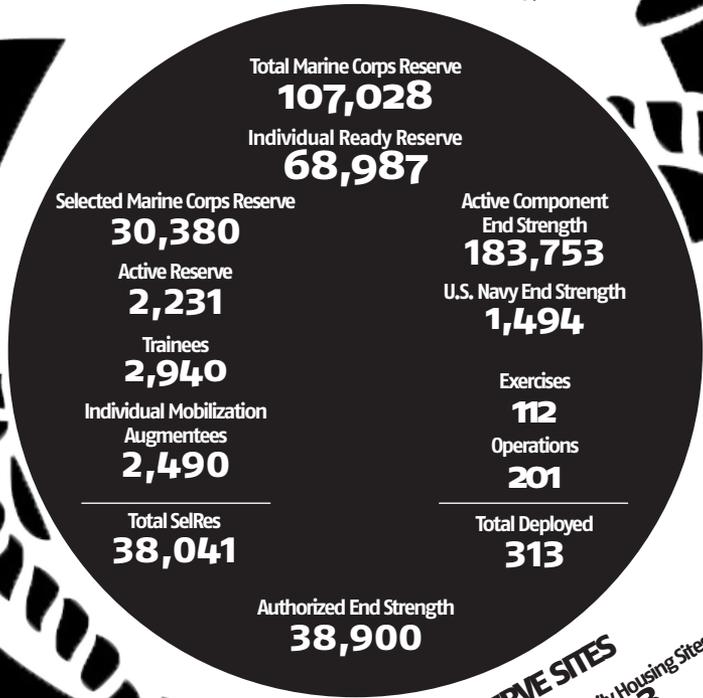
Commander, Marine Forces Reserve

The cyber domain is just as much a part of our battlespace as the air, land, or sea. Being cognizant of the ever-present cybersecurity risk is equally as important as our physical security and force protection efforts. Cybersecurity threats are nothing new, but they are on the rise.

Last year the Office of Personnel Management experienced two separate hacking incidents that compromised the personal information of millions of service members and their families. More recently, there has been at least one phishing attack on MARFORRES.

Phishing attacks are attempts by adversaries to capture personal information through deception. One example is manipulated email purporting to be from the Marine Corps, or from some other trusted organization, that attempts to extract sensitive information from the email recipient.

These hacking attempts have been around for several years, and they can be devastating. Being knowledgeable about what they are, how to prevent them, and how to report them is critical to cybersecurity. I expect all Marines and Sailors to learn about this threat and be prepared to combat it. Semper Fidelis.



**RESERVE SITES**  
 Tenant Locations **133**  
 Owned Sites **27**  
 Family Housing Sites **3**

Click on the names below to view the bios and photos

# LEADERSHIP

Secretary of the Navy	Hon. Ray Mabus
Commandant of the Marine Corps	Gen. Robert B. Neller
Assistant Commandant	Gen. John M. Paxton Jr.
Sergeant Major of the Marine Corps	Sgt. Maj. Ronald L. Green
Commander, Marine Forces Reserve	Lt. Gen. Rex C. McMillian
Executive Director, Marine Forces Reserve	Mr. Gregg T. Habel

Sergeant Major, Marine Forces Reserve	Sgt. Maj. Anthony A. Spadaro
Command Master Chief, Marine Forces Reserve	CMDCM Chris Kotz
4th Marine Division	Brig. Gen. Paul K. Lebidine
4th Marine Aircraft Wing	Maj. Gen. William T. Collins
4th Marine Logistics Group	Brig. Gen. Patrick J. Hermesmann
Force Headquarters Group	Brig. Gen. Helen G. Pratt



# Reporting Phishing and Malicious Email Messages Received



## What is Phishing?



Phishing is the attempt to gather information from the recipient through a legitimate-looking email from a fraudulent sender.

It is imperative you report any suspected malicious email sent to your usmc.mil account and that you do not open any suspected email sent to your personal account (e.g., Gmail) on a government computer. This guide is provided to help you prevent hackers from successfully attacking our network.

## Identification

### 1. Hover over "From"

If you are accessing your personal email from work, you can identify the sender by hovering your mouse arrow over the name in the "From" column. This will give you the sender's email address. If it does not match the sender's name, it is probably a malicious email.

### 2. Are the URLs legitimate?

Another way to "hover" check would be any URLs the email is directing you to visit. Always ensure the link is legitimate and uses encryption (<https://>).

### 3. Request for personal information

One commonly used tactic is an urgent request to update your personal information (e.g., Social Security number, bank account details, account password). Phishers use this tactic to drive someone to a malicious URL or download an attachment aiming to infect the user's computer or steal their information.

### 4. Incorrect grammar/spelling

A common practice of many hackers is to use misspelled words on purpose. While it may seem that this would easily reveal an illegitimate email, it is actually a tactic used to find less savvy users.

### 5. Message body is an image

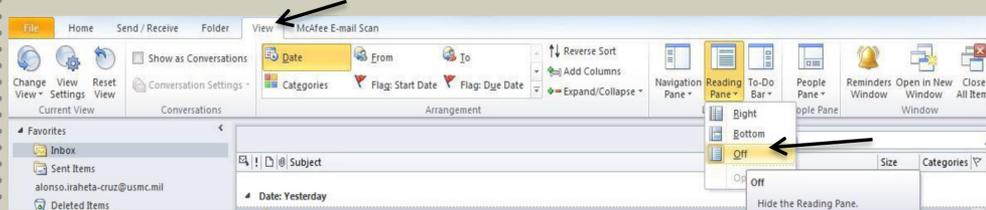
This is a common practice of many spammers. The images may contain hyperlinks that navigate you to infected websites.

### 6. Suspicious attachments

Most financial institutions or retailers will not send out attachments via email. High-risk attachment file types include: .exe, .scr, .zip, .com, .bat, among others. Check links by hovering the cursor over the image to ensure that it is sending you to a legitimate website. Or, open a new window and type the address you already have for your financial institution or retailers.

## Preventive Measures

### 1. Turn off the Microsoft Outlook reading pane.



### 2. Only open attachments or navigate to sites in emails that are digitally signed.



## Reporting Instructions

1. Submit a trouble ticket to the G6 Service Desk by calling (504) 697-7777. You will be assigned a trouble ticket number.

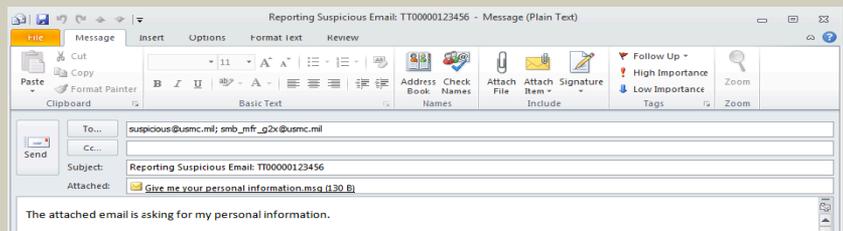
2. Report suspicious email by attaching the original message as a file. DO NOT forward the email, as this will remove specific details necessary to track the origin of the message.

a. Click on the new email icon, opening a new message.

b. Without opening the original message, right click on it and select "copy."

c. Right-click in the blank content area of the new blank email and select paste from the pop-up menu.

d. Type "Reporting Suspicious Email:" followed by the ticket number in the subject line.



e. Address the email to suspicious@usmc.mil and smb\_mfr\_g2x@usmc.mil and include why the email is suspected of being suspicious. Dont forget the underscores if typing the email address yourself!

f. Click "Send."