



CRIMINAL INVESTIGATION DIVISION

MCIPAC – MCB CAMP BUTLER | PUBLIC BULLETIN



ONLINE FINANCIAL SCAM ALERT

(U) SITUATIONAL AWARENESS:

In 2020, the MCIPAC Criminal Investigation Division conducted multiple investigations regarding fraudulent use of bank account information. Recently, suspects have hacked profiles on social media outlets to entice service members by offering “fast cash” in the following phishing schemes:

Top Trends of Phishing



Trend #1: Victims were contacted via Instagram, Facebook Messenger, and/or Snapchat from a profile posing to be a Marine and asked if they were interested in earning money. Suspects then request the victim’s personal banking account information such as **username and password** with a promise that a large sum of money will be deposited into their banking account. Specifically, the suspect claimed his uncle owns a construction business that gets a grant from the government, and he can add the victim onto the payroll. The victim is promised to get a cut of that grant money typically through Navy Federal Credit Union (NFCU). Victims who have given their username and password have been locked out of their account.

Trend #2: Victims were contacted via Instagram, Facebook Messenger, and/or Snapchat from a profile posing to be a Marine and asked if they are interested in earning money. Suspects then request the victim’s picture of the **front and back of their debit card** with a promise that a large sum of money will be deposited into their banking account, typically through NFCU.

Trend #3: Individuals would contact an **advertisement page** via Instagram, Facebook Messenger, and/or Snapchat containing a promise to earn fast cash. After the initial contact the suspect uses one of the two schemes which are listed above.

Trend #4: Victims have been contacted through an **email asking to change their apple password**, which will require an email address and an old password. Once you plug in the information you will be directed to a different screen that ask for your credit card number and social security number.

In all cases, the victims were unaware that personal loan was taken out in their name, which appeared as a large deposit. They were then requested or threatened to withdraw the lump sum or a percentage of the deposit and send it in cash via the United States Postal Service, Apple Pay or Cash App. Moreover, the aforementioned loans were over \$10,000, which the victims had to pay back!

(U) THE CRIMINAL INVESTIGATION DIVISION ADVISES THE FOLLOWING:

- Do not give out your personal financial information.
- Do not add or accept friend/follower requests from people you don’t know.
- The bank will never contact you to request your secure login information.
- Solicitation through social media to obtain banking information, to receive “fast cash,” is not to be considered a genuine method for earning wages.
- If you or someone you know was a victim of a financial fraudulent scheme, please contact your local PMO office.
- If your social media friend contacts you about “fast cash” they were hacked.

NFCU AND OTHER FINANCIAL INSTITUTIONS WILL NOT REIMBURSE INDIVIDUALS WHO WILLINGLY DISCLOSE THEIR FINANCIAL INFORMATION. CONTACT YOUR FINANCIAL INSTITUTION FOR OTHER TIPS.

*****If you believe fraud has occurred, call your financial institution immediately to put a hold on your account. Navy Federal members can call the 24-hour service line at 1-888-842-6328. *****