





## ADVISORY

### ARMY NATIONAL GUARD (ARNG) Defensive Cyber Operations – National Guard (DCO-NG)

#### BEST PRACTICES

##### Precautions to Help You Avoid Becoming a Victim

- Monitor financial account statements and immediately report any suspicious or unusual activity to financial institutions.
- Request a free credit report at [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling 1-877-322-8228. Consumers are entitled by law to one free credit report per year from each of the three major credit bureaus – Equifax®, Experian®, and TransUnion® – for a total of three reports every year.
- Consider placing a credit freeze on your credit report with each of the credit bureaus.
- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about you, your employees, your colleagues, or any other internal information.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Do not send sensitive information over the Internet before checking a website's security. For more information, see [Protecting Your Privacy](#).
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the [Anti-Phishing Working Group](#).
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic. For more information, see [Understanding Firewalls](#); [Understanding Anti-Virus Software](#); and [Reducing Spam](#).
- Take advantage of any anti-phishing features offered by your email client and web browser.
- Employees should take steps to monitor their personally identifiable information and report any suspected instances of identity theft to the [FBI's Internet Crime Complaint Center](#).

#### REFERENCES

##### OPM Identity-Protection Phishing Campaigns

<https://www.us-cert.gov/ncas/current-activity/2015/06/30/OPM-Identity-Protection-Phishing-Campaigns>

##### Security Tip (ST04-014) Avoiding Social Engineering and Phishing Attacks

<https://www.us-cert.gov/ncas/tips/ST04-014>

##### OPM.gov Latest News and Announcements

<https://www.opm.gov/news/latest-news/announcements/>

##### FTC Credit Freeze Frequently Asked Questions

<http://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>

If you have any questions about this notification, contact:

**Defensive Cyber Operations – National Guard**  
[ng.ncr.ngb.mbx.dco-ng-cnd@mail.mil](mailto:ng.ncr.ngb.mbx.dco-ng-cnd@mail.mil)