OPM Cybersecurity Incident Update #2 – 15 June 2015

Point of Contact: HRPolicy@aafes.com

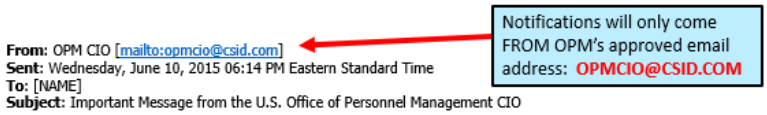
Fellow associate,

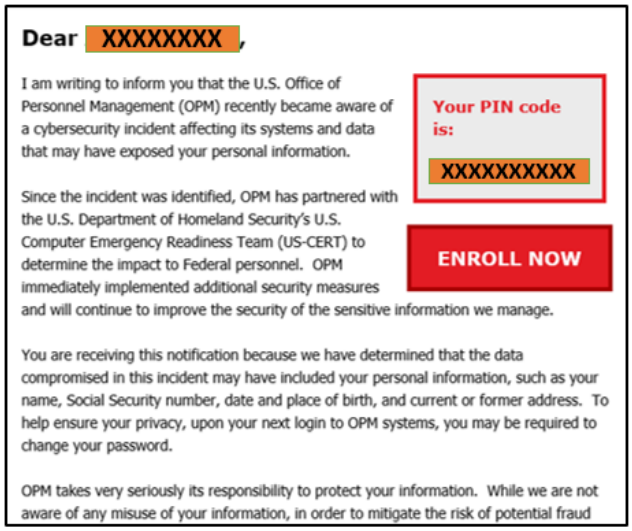
On 5 June 2015, we advised you of the OPM data security breach that affected some current and former federal employees. As a reminder, this breach did not impact the personnel records of Exchange associates – Exchange personnel records are maintained internally. However, if you have former federal employment and you have been contacted by the OPM, here is what the information will look like.

In the coming weeks, OPM will be sending notifications to individuals whose Personally Identifiable Information (PII) was potentially compromised in this incident. **The email will come from opmcio@csid.com and it will contain information regarding credit monitoring and identity theft protection services being provided to those Federal employees impacted by the data breach.** In the event OPM does not have an email address for the individual on file, a standard letter will be sent via the U.S. Postal Service.

As a note of caution, confirm that the email you receive is, in fact, the official notification. It's possible that malicious groups may leverage this event to launch phishing attacks. To protect yourself, we encourage you to check the following:

1. Make sure the sender email address is "opmcio@csid.com."
2. The email is sent exclusively to your work email address. No other individuals should be in the To, CC, or BCC fields.
3. The email subject should be exactly "Important Message from the U.S. Office of Personnel Management CIO."
4. Do not click on the included link. Instead, record the provided PIN code, open a web browser then manually type the URL http://www.csid.com/opm into the address bar and press enter. You can then use the provided instructions to enroll using CSID's Web portal.
5. The email should not contain any attachments. If it does, do not open them.
6. The email should not contain any requests for additional personal information.
7. The official email should look like the sample screenshot below





Additional information has also been made available beginning on 8 June 2015 on the company's website and by calling toll-free 844-777-2743 (International callers: call collect 512-327-0705).

Regardless of whether or not you receive this notification, employees should take extra care to ensure that they are following recommended cyber and personal security procedures. If you suspect that you have received a phishing attack, contact your agency's security office.

In general, government employees are often frequent targets of "phishing" attacks, which are surreptitious approaches to stealing your identity, accessing official computer systems, running up bills in your name, or even committing crimes using your identity. Phishing schemes use email or websites to trick you into disclosing personal/sensitive information.

We will continue to keep you advised of new developments regarding this cyber-security incident as we learn more from OPM. Click here for tips on monitoring your identity and financial information and precautions to help you avoid being a victim.

Steps for Monitoring Your Identity and Financial Information

- Monitor financial account statements and immediately report any suspicious or unusual activity to financial institutions.
- Request a free credit report at 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. Contact information for the credit bureaus can be found on the Federal Trade Commission (FTC) website, www.ftc.gov.
- Review resources provided on the FTC identity theft website, www.Identitytheft.gov. The FTC maintains a variety of consumer publications providing comprehensive information on computer intrusions and identity theft.
- You may place a fraud alert on your credit file to let creditors know to contact you before opening a new account in your name. Simply call TransUnion® at 1-800-680-7289 to place this alert. TransUnion® will then notify the other two credit bureaus on your behalf.

Precautions to Help You Avoid Becoming a Victim

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about you, your employees, your colleagues or any other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- 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, http://www.us-cert.gov/ncas/tips/ST04-013).
- 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 (http://www.antiphishing.org).
- 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 at www.ic3.gov.
- Additional information about preventative steps by consulting the Federal Trade Commission's website, www.consumer.gov/idtheft. The FTC also encourages those who discover that their information has been misused to file a complaint with the commission using the contact information below.

Identity Theft Clearinghouse

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
https://www.identitytheft.gov/
1-877-IDTHEFT (438-4338)
TDD: 1-202-326-2502