

---

**From:** Celia Esposito-Noy <Celia.Esposito-Noy@solano.edu>  
**Sent:** Friday, April 29, 2016 6:24 PM  
**To:** \$ALL  
**Subject:** FAQ regarding W-2 phishing incident

**Importance:** High

### **W-2 Phishing Incident Frequently Asked Questions (FAQ)**

#### ***What happened?***

On April 28<sup>th</sup>, an employee of the college was “spoofed” and provided W-2 information for all SCC employees who worked for the college in 2015. The information on the W-2 forms included names, social security numbers, annual amount earned, and amounts deducted for federal, state, and retirement contributions. Birthdates, names of dependents, and bank accounts **were not** included. The spoofed email came from an external environment, the Solano County Computer Crimes Task Force was notified and is investigating the source. Our IT staff also responded quickly to identify the email address of the sender and assisted the task force. All legal avenues are being used to locate and, if possible, prosecute those involved.

#### ***What should I do now?***

While we have received no reports that this information has been misused in any manner, as a precaution, we are offering affected employees with **a free, one-year membership in Experian’s® ProtectMyID® Alert**. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. We encourage you to take advantage of the identity theft protection services being offered. Further, you should remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity.

The State of California Department of Justice provides the best guidelines for the steps you should take to protect your identity. Go to <https://oag.ca.gov/idtheft/facts/freeze-your-credit> for step-by-step information.

#### ***Do I need a code to sign up for credit monitoring services?***

Credit monitoring is being provided to all affected individuals. In order to enroll in the credit monitoring services, you will need the activation code that will be included in the letters mailed to affected individuals. You will also be provided an activation code by email early next week.

#### ***What is “spoofing?”***

Email spoofing is the creation of email messages with a forged sender address. Spam and phishing emails typically use such spoofing to mislead the recipient about the origin of the message”

([https://en.wikipedia.org/wiki/Email\\_spoofing](https://en.wikipedia.org/wiki/Email_spoofing), accessed 4/28/16).

#### ***What is a phishing email?***

Phishing is the attempt to acquire sensitive information, such as usernames, passwords, and credit card details, often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by email, and it often directs users to enter details at a fake website that looks and feels similar to a legitimate one.

#### ***Who was affected?***

Anyone employed by SCC in 2015 was impacted including student workers, temporary employees, adjunct faculty, and full time employees. Affected individuals will receive notification by U.S. Mail regarding this incident and advised of the steps they can take to protect themselves. We will have information available on our home page and a designated email account has been established where questions can be sent. You can also call 707-863-7897 Monday-Friday from 9:00am-4:00pm. See My Solano for updates.

***How do we avoid this from happening again?***

All employees will be receiving additional education and training regarding “phishing” emails, and we are conducting a comprehensive review of our security practices, procedures and safeguards. This is an opportunity for us to improve our security protocols.

***How do I place a security freeze?***

If you choose, you may place a security freeze through the credit bureaus in addition to the ProtectMyID option that the college will pay for. According to the Office of the Attorney General, “To place a freeze, you must contact each of the three credit bureaus. You can request the freeze by mail. You may also place the freeze online. Here are the freeze web pages for the credit bureaus. Note: If these links do not work, search "security freeze" on the credit bureau web sites.

<https://www.freeze.equifax.com>

<https://www.experian.com/freeze/center.html>

<http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page>”

In the state of California, a security freeze is free to identity theft victims who have a police report of identity theft. We will provide a copy of the police report to affected individuals as soon as the report is available.

If you are not an identity theft victim and you are under 65 years of age, it will cost you \$10 to place a freeze with each of the three credit bureaus. That is a total of \$30 to freeze your files. If you are not an identity theft victim and you are 65 years of age or older, it will cost you \$5 to place a freeze with each of the three credit bureaus. If you have already paid to have a credit freeze placed with the credit bureaus, please keep your receipts and SCC will create a process for reimbursement.

The crime report is available at My Solano. You will be asked to provide a copy of the crime report to get a security freeze at no charge.

***Where can I find more information on placing a security freeze and other steps to take to protect my identity?***

The Office of the Attorney General provides extensive information at <https://oag.ca.gov/idtheft/facts/freeze-your-credit>. Additionally, we will continue to post notices at My Solano and send updates using the SCC email.

*Celia Esposito-Noy, Ed.D.*  
*Superintendent-President*  
*Solano Community College*  
*(707) 864-7299*  
[Celia.Esposito-Noy@solano.edu](mailto:Celia.Esposito-Noy@solano.edu)

