Zipcar Arrives At SSU!

Zipcar is finally here! Sonoma State students (over 18 years of age), faculty and staff can use a new car sharing service called Zipcar! Zipcar is widely used throughout the San Francisco Bay Area and is now available at Sonoma State University. The designated pick up and drop areas for the Zipcars will be located in the two spaces at the northwest corner of D lot across from the Police and Safety Services building. Zipcar is car-sharing an alternative to car ownership that gives members 24/7 access to vehicles parked right on campus. Their low hourly and daily rates include gas, insurance, and 180 miles per day to get you to wherever you want to go. Members can reserve Zipcars online or with a smart phone for use lasting an hour or up to seven days. You can enjoy all the freedom of owning car without any of the hassle. Zipcars are not to be used for official University travel. To learn more about the Zipcar program please visit: www.zipcar.com/universities/sonoma-state

Coming Soon To SSU: Electric Vehicle Charging Stations!!!!

In an effort to help improve air quality by offering an alternative fuel source, and to further support the use of electricity powered vehicles, Sonoma State University is preparing to move forward with installing three Type-2 Electric Vehicle (EV) charging stations in D lot and two chargers in L lot. Anyone with a valid SSU parking permit can use the EV charging stations. Users of the EV charging stations will be limited to 4 hours of charging time per charging session. Parking Services personnel will monitor the charging stations for compliance. It is anticipated that the installation of the charging stations will be completed during Spring/Summer of 2016. Additional information will be posted on line at: www.sonoma.edu/ps/transportation

Did You Know.....
“Crime Prevention Is The Technique of Reducing or Eliminating Opportunities For Crime.”
Radioactive Waste Management and Safe Storage

Radioactive waste is a byproduct of nuclear processes and can pose dangers if not handled properly. Efficient waste management is crucial to protect the health and safety of workers and the environment. The SSU Office of Information Security plays a key role in safeguarding confidentiality, integrity and availability of sensitive information, critical systems, and other important information. We took a minute to ask Andru Luvisi, Information Security Officer, for questions related to Information Security.

Q: What is the role of the Information Security Officer?
A: My primary focus is to track and protect sensitive data and design and deploy more secure systems.

Q: What is sensitive data/information?
A: Sensitive data includes Social Security numbers, dates of birth, driver’s license numbers, bank accounts and medical information.

Q: What are some common breaches in Information Security and how do they occur?
A: Phishing and Malware. Phishing is attempting to deceive a victim into disclosing sensitive information to the criminal. For example, an email might encourage you to click on a link that seems to take you to your bank’s login screen, but is actually taking you to a web site run by the criminal. Malware (Malicious Software) is software that runs on your own device and acts in the interests of others to compromise your personal information. You can be infected with malware by opening a malicious attachment to an email, by downloading and running a piece of malware (often masquerading as desirable software), or by having a vulnerability in one of your programs be exploited by an attacker.

Q: What can people do to protect sensitive data?
A: Never click on suspicious links within an email or anywhere else and keep your computer devices up to date with the latest security patches. People can contact the ISO for more information. The ISO email address is: iso@sonoma.edu

Mail and Phone Scams On The Rise

SSU Police Services has noted an increase in mail and telephone scams from criminals posing as the Internal Revenue Service (IRS) or prospective employers intending to trick victims out of their money and personal information.

Please note that the IRS will not:

- Demand that you provide payment via a certain method (i.e. debit or credit card).
- Ask for your credit or debit card numbers over the phone.
- Threaten to send the police or other agencies to arrest you for failing to make payments.
- Demand that you pay outstanding debt immediately without consulting a tax professional.

Please also note that legitimate prospective employers will not:

- Send you a check via the mail and ask you to deposit it and send a large portion of it to an unknown mailing address.
- Send you a paycheck for more than your salary and ask you to mail them the difference in a separate check or money order.

Residential Crime Prevention Tips

Help Police Services help You. Please follow the below tips to reduce the likelihood of becoming a victim of a residential crime:

>Lock doors and windows, particularly when you depart
>Don’t leave valuables in view from windows
>Don’t write identifying information on card access keys
>Don’t open the door for strangers
>Introduce yourself to neighbors to encourage communication and awareness within the community
>Report suspicious people to SSU Police Services

New Law Regarding ‘Hoverboards’

A Hoverboard is defined, in part, as “an electrically motorized board/wheeled device that has a floorboard designed to be stood upon when riding that is not greater than 60 inches deep and 18 inches wide, is designed to transport only one person, and has an electric propulsion system averaging less than 1,000 watts.” Effective January 1, 2016, and pursuant to sections 21291 and 21292 of the Calif. Vehicle Code, Hoverboards can only be operated by persons 16 years of age or older. Riders must wear a properly fitted and fastened helmet. Violators may be issued a citation payable through the Sonoma County Traffic Court. Additionally, Hoverboards are not permitted in the SSU Res. Halls.

4 Questions With The SSU Information Security Officer

The SSU Office of Information Security plays a key role in safeguarding confidentiality, integrity and availability of sensitive information, critical systems, and other important information. We took a minute to ask Andru Luvisi, Information Security Officer, for questions related to Information Security.

Q: What is the role of the Information Security Officer?
A: My primary focus is to track and protect sensitive data and design and deploy more secure systems.

Q: What is sensitive data/information?
A: Sensitive data includes Social Security numbers, dates of birth, driver’s license numbers, bank accounts and medical information.

Q: What are some common breaches in Information Security and how do they occur?
A: Phishing and Malware. Phishing is attempting to deceive a victim into disclosing sensitive information to the criminal. For example, an email might encourage you to click on a link that seems to take you to your bank’s login screen, but is actually taking you to a web site run by the criminal. Malware (Malicious Software) is software that runs on your own device and acts in the interests of others to compromise your personal information. You can be infected with malware by opening a malicious attachment to an email, by downloading and running a piece of malware (often masquerading as desirable software), or by having a vulnerability in one of your programs be exploited by an attacker.

Q: What can people do to protect sensitive data?
A: Never click on suspicious links within an email or anywhere else and keep your computer devices up to date with the latest security patches. People can contact the ISO for more information. The ISO email address is: iso@sonoma.edu

Thank You For Supporting the Dismount Zone Program

ONLY 19 CITATIONS ISSUED TO DATE