SDSU SAFETY & SECURITY NEWSLETTER

OCTOBER 2017

EM CONTACT INFORMATION
Morrill Hall 208A, Box 2201
(605) 688-4251

Jayme Trygstad
Emergency Management Specialist
jayme.trygstad@sdstate.edu

Emergency Preparedness is a Team Sport."
–Eric Whitaker

Always remember…
each one of you is a safety officer:
If You See Something Say Something!

EMERGENCY MANAGEMENT

We are all dedicated to crime prevention year round, but during October, which is Crime Prevention Month, we would like to highlight efforts to make our community safer from crime and violence.

Reminder that the Jackrabbits Guardian App is a way to report any suspicious activity to the SDSU Police Department. I want to encourage staff members to download the app and take the time to show one student how it works and encourage them to download the app.
Tip Texting – Crowd Sourced Safety is 2-way tip texting that encourages you to get involved when you see something. It's a cost effective addition of "eyes and ears" to your security operations. With the tip submission feature, users can discreetly submit 2-way tips with text and images to report suspicious behavior, potential problems, and other hazards. The University Police Department receives geo-tagged tips in real time, allowing them to respond instantly with two-way messaging.
Emergency Call Button is a pre-configured for calls and text tips with UPD from your mobile phone. It automatically delivers a caller safety profile – including your current location.
Safety Timer – Automatic Check-in gives users a virtual escort and keeps them safe and connected to UPD or your Guardian. Users set their Safety Timer with a time and destination to confirm their safe arrival. While the Safety Timer is active, UPD or your Guardian can check the app user's status and location.

National Teen Driver Safety Week
Parents can help by talking to your teen drivers about the rules of the road. Parents can take a simple step to help protect their teen drivers from these tragedies by talking with their teenagers about ways to reduce some of the risks when their teens are behind the wheel. Additional information

National Weather Service started on October 1st using a HazSimp, which is Hazard Simplification to explain the simplification of current watch/warning/advisory products. Now when a threat is issued the NWS will use What, Where, When, Additional Details, and

Precautionary/Preparedness Actions in the information given so you can quickly final all the information about a threat.
Also a reminder to sign up for the apps to receive the information from the NWS with Winter weather quickly approaching.
Additional Information

I am now a Weather-Ready Nation (WRN) Ambassador from the National Weather Service. What does that mean for SDSU? I will continue to work with the National Weather Service to help build a campus that is ready, responsive, and resilient to the impacts of extreme weather and water events. An ambassador is committed to Promoting Weather-Ready Nation messages and themes to our campus community, engaging with NOAA personnel on potential opportunities, and serving as an example by educating employees on workplace preparedness. SDSU extension has been a WRN and once approved the main campus will be recognized as well.

As we build on our education to the campus community about such events, this will become a recognition that we can display proudly.
Additional Information

Jayme Trygstad

EHS Contact Information
Avera Health Services
Room 143, Box 2202
(605) 688-4264
Fax (605) 688-4290
ehs@sdstate.edu

Dr. Gary Yarrow
Director
gary.yarrow@sdstate.edu

Joshua Mann
Assistant EHS Officer
joshua.mann@sdstate.edu

ENVIRONMENTAL HEALTH & SAFETY

Laboratory Safety

The biggest solution to laboratory safety is to lock your doors, just like locking your house or your car. Labs can contain a variety of easily removed items such as chemicals, scales, computers, cell phones and all the myriad other expensive lab supplies. It is critical that all laboratory areas maintain security at all times: *especially when the lab is unattended and always at night, even when attended.* SDSU is a safe place to work and learn, but unlocked doors can be an invitation to people that have no business coming into the laboratory.

Whenever you are working in a restricted area (even somewhat restricted) and you see someone that you don't think belongs there, ask them their name and which lab they are working. If you are in the building or lab alone, don't confront them but go to your office or lab and call the University Police Dept. (688-5117). They probably do belong there but do not take chances, let security handle it.

Cont…

Research or other activities in laboratories involving lab space, materials or equipment is not allowed unless approved by the lab's PI: if you find someone using equipment that you don't recognize, ask.
Never prop outside doors open at any time. This is an invitation for uninvited persons, as well. Never prop laboratory doors open, especially after hours. If someone is meant to be there, they will have approved access and keys. When leaving your lab at night and you feel uncomfortable, take advantage of the university after hours assistance by calling the University Police Dept. (688-5117).

As part of laboratory security, be sure that your data is secured, backed up and in your control.

Let's be safe and secure out there!

Dr Gary Yarrow

Kenneth Larson
Assistant EHS Officer
kenneth.larson@sdstate.edu
Tina Brown
Senior Secretary
and
Campus Ergonomic Representative
tina.brown@sdstate.edu

For after-hours assistance,
contact the
University Police Department
at 688-5117

In an emergency,
dial 111 from a campus phone
or
911 from a cellular phone.

UNIVERSITY POLICE DEPARTMENT

UPD Contact Information
1405 Jackrabbits Avenue
Box 2920
(605) 688-5117
Fax (605) 688-4636
sdsu.upd@sdstate.edu

Chief Tim Heaton
timothy.heaton@sdstate.edu

Deputy Chief Michael Kilber
michael.kilber@sdstate.edu

Sergeant William Taylor
Operations
william.taylor@sdstate.edu

The University Police Department recommends that you never leave your laptop unattended in a public place. If you take your laptop to classrooms, conference rooms or even offices, do not leave it alone. Not even for a minute. Opportunistic thieves could be lurking in the shadows. If you do leave your laptop in a public place, lock it up with a notebook cable lock or other security device. Physical locks are the best means to prevent your laptop from being stolen. Most stolen laptops are grabbed and gone before their owners know what happened. Laptop thieves look for quick easy hits, and will not risk the delay or commotion of trying to break a lock.

Even if you stay with your laptop avoid setting it on the floor. Putting your laptop on the floor is an easy way to forget or lose track of it. If you have to set it down, try to place it between your feet or against your leg so you're always aware of it. Also consider using a shoulder bag, briefcase, or backpack for your laptop. Avoid expensive bags that might draw in would-be thieves.

If you must leave your laptop in a car, stow it cased in the trunk before you reach your destination so potential thieves don't see you and make sure your car is locked.

Sergeant Jon Anderson
jonathan.anderson@sdstate.edu

For Emergencies
call 111 from a campus phone.

Emergency calls using 911 will be transferred from the Brookings Police Department to the UPD Communications Center.

If you leave your door open, you are providing thieves easy access to steal your belongings and equipment that belongs to SD State.
If you are leaving for a significant amount of time, lock your office. Many laptops and internet devices are stolen from offices, while the occupant is on a quick break or at a meeting. And of course many offices have desktop computer to secure as well. Just because it has cables coming out of the back does not mean a thief won't be interested.
Of course all computers should be set to require a password to log on to the computer. Never leave access numbers or passwords in your carrying case, on your desk, under your keyboard or other places easy to find.

We also recommend never allowing your web browser to automatically record and supply a password for you. If you do, it means that anyone at your computer can access that site under your account.

And finally please report any lost or stolen computers or internet devices to both IT and the University Police Department immediately. Any delay or hesitation benefits the thief, could result in stolen data and reduces the chances of the computer being recovered.

Chief Tim Heaton

Information Security Office

Ryan Knutson
Ass't Vice President
for Technology
ryan.knutson@sdstate.edu
Office: Morrill Hall 208B
Phone: 688-4988

Mavhu Chidaushe
Information Security Officer
mavhu.chidaushe@sdstate.edu
Office: Morrill Hall 117
Phone: 688-6912

CYBER SECURITY

What You Should Know About the 'KRACK' Wi-Fi Security Weakness

Researchers this week published information about a newfound, serious weakness in **WPA2**— the security standard that protects all modern Wi-Fi networks. What follows is a short rundown on what exactly is at stake here, who's most at-risk from this vulnerability, and what organizations and individuals can do about it. Short for **Wi-Fi Protected Access II**, WPA2 is the security protocol used by most wireless networks today. Researchers have discovered and published a flaw in WPA2 that allows anyone to break this security model and steal data flowing between your wireless device and the targeted Wi-Fi network, such as passwords, chat messages and photos. "The attack works against all modern protected Wi-Fi networks," the researchers wrote of their exploit dubbed "KRACK," short for "Key Reinstallation AttaCK.

Read more about it at http://krebsonsecurity.com/

SDSU Information Security and Network Team is working with vendors to deal with this vulnerability and have an action plan in place once patches have been made available. We will be announcing any planned outages on InsideState in the next coming weeks.

Cont…

Laramie Meyer
Sr. Computer Support Specialist
laramie.meyer@sdstate.edu
Office: Morrill Hall 117B
Phone:688-5941

Contact us if you have questions!

See our website on InsideState: https://insidestate.sdstate.edu/technology/infotech/Units/infosec/default.aspx

Did you know that typing the wrong url into a browser leads you to malicious websites? Can't install an app? Ask us about whitelisting it! We are here to help you stay secure!

Securing The Human Training

Just a reminder that security awareness training is available via Securing the Human. For any issues please contact the SDSU Support Desk at SDSU.SupportDesk@sdstate.edu

Equifax Breach Updates

October 12 Equifax Credit Assistance Site Served Spyware
October 10 Equifax Hackers Stole Info on 693,665 UK Residents
October 8 Equifax Breach Fallout: Your Salary History

Cyber Security Tips for the Holiday Season

Proceed with caution at retail locations that do not accept Chip-card transactions.

- If you encounter a point-of-sale terminal with a note covering the slot saying "no Chip cards" or "must swipe", consider using cash instead of a card – or, consider a smartphone payment option such as Apple Pay or Android Pay.
- If cash or smartphone payment is not an option, use a credit card as opposed to a debit account. If your debit card information is compromised in a data breach, criminals can drain your checking account with no guarantee you will recover all of the funds.

Enable transaction notifications through online banking and smartphone apps.

- Set up alerts with your bank and credit providers to be notified in the event of unauthorized transactions or certain activities, such as charges over $100.
- Many financial institutions now offer the option to receive a text message or smartphone app alert every time a transaction is charged to your account.

Take advantage of credit monitoring or identity theft insurance, when offered.

- If your data was compromised in one of the many breaches that occurred over the last two years, sign up for any free credit monitoring or identity theft insurance services offered by the company. If you are eligible for coverage, you should have received a letter in the mail with information. You can always search for past data breaches by querying a search engine for the company name + "data breach".
- For additional information, visit the Identity Theft Resource Center.

Enable two-factor authentication (2FA) on all financial, email, and online shopping accounts.

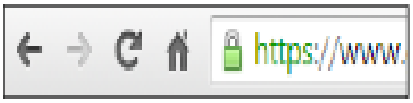
- If a website offers 2FA, be sure to enable it as it will prevent criminals from gaining access to your accounts, even if they obtain the password.

- Check out this site for an extensive list of websites that offer 2FA: https://twofactorauth.org

Perform basic “cyber-hygiene” on all devices used for shopping, banking, etc.

- Keep your operating system and all software applications updated.
- Download antivirus/antispyware software and set it to update automatically.
- Confirm that your firewall is enabled and configured to a secure setting.
- Secure your home Wi-Fi signal with a strong password.
- Remove any unnecessary software/apps and avoid downloading apps from untrusted sources.
- Check out “Ten Ways to Improve the Security of a New Computer” from US –CERT.

Look for “HTTPS” and a lock symbol in the URL field of your browser when shopping or banking online.



- The “s” in “HTTPS” stands for “secure” and indicates that communication with the webpage is encrypted.
- Do not enter any login credentials or personal/financial information into any website that does not display this security feature.

Report any suspicious activity or malicious cyber activity.

- Citizens: If you are the victim of identity theft, financial fraud, or malicious cyber activity, report it to your local police department immediately and obtain a case number.
- Consider reporting cyber incidents to the FBI IC3 here.
- For identity theft, contact the three credit bureaus and file a report with each of them.

Be cyber safe!

Mavhu Chidaushe