



CYBERSECURITY AWARENESS MONTH



Stay Safe @ Home: Cyber Security Tips and Tricks for Home and Work



Date: Wednesday, October 21, 2020
Presenter: Mary Morshed, Campus ISO



Do Your Part. #BeCyberSmart

OCTOBER MEANS...

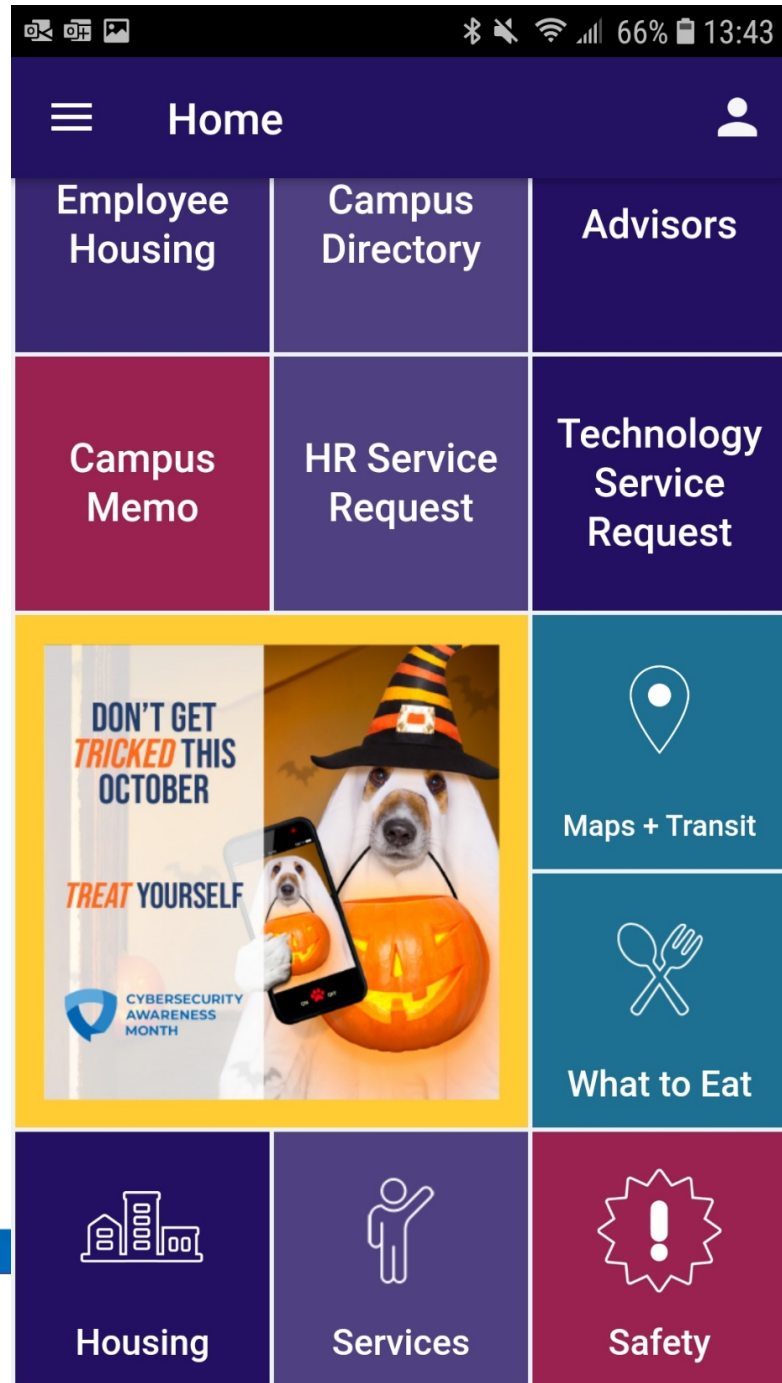
1. HALLOWEEN
2. PUMPKIN SPICE LATTES
3. CYBERSECURITY AWARENESS MONTH



[STAYSAFEONLINE.ORG /
CYBERSECURITY-AWARENESS-MONTH](https://staysafeonline.org/cybersecurity-awareness-month)



SF State's Mobile App
Spotlight Item
October 21st – 24th

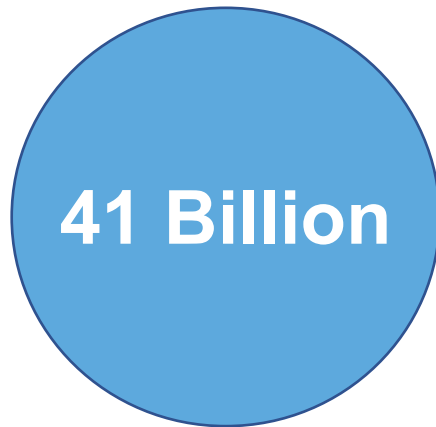


Do Your Part. #BeCyberSmart

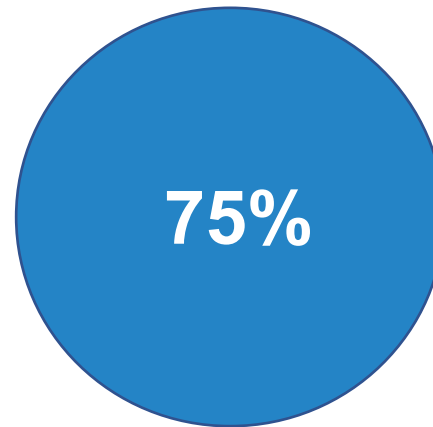


If You Connect It, Protect It.

Cybersecurity Awareness Month 2020 is about taking proactive steps to enhance cybersecurity at home and in the workplace



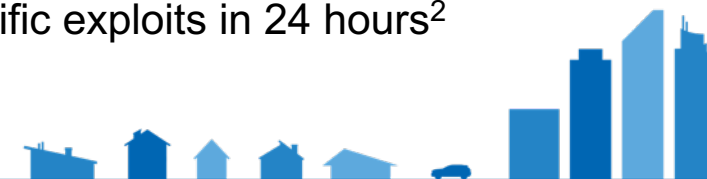
There will be more than 41 billion IoT devices by 2027, up from about 8 billion in 2019³



75% of infected devices in IoT attacks are routers¹



Once plugged into the internet, connected devices are attacked within 5 minutes and targeted by specific exploits in 24 hours²



¹ Symantec: <https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/istr-2019-internet-things-cyber-attacks-grow-more-diverse>

² NETSCOUT Threat Intelligence Report: https://www.netscout.com/sites/default/files/2019-02/SECR_001_EN-1901%20-%20NETSCOUT%20Threat%20Intelligence%20Report%20H%202018.pdf

³ Business Insider Intelligence: <https://www.businessinsider.com/internet-of-things-report?IR=T>

Do Your Part. #BeCyberSmart

Weekly Focus Areas



<https://its.sfsu.edu/announcement/cybersecurityawarenessmonthoctober2020>

October 1-4	Official Cybersecurity Awareness Month Kick-off
Week of October 5	If You Connect It, Protect It
Week of October 12	Securing Devices at Home & Work
Week of October 19	Securing Internet-Connected Devices in Healthcare
Week of October 26	The Future of Connected Devices



Do Your Part. #BeCyberSmart

Working/Learning Remotely Cyber Security Challenges



Cyber Security is more important than ever

- No longer connecting to protected networks
- Increased phishing emails; Attackers know everyone is working/learning remotely
- Distractions lower our radar for identifying suspicious emails and suspicious technical behaviors



Own Your Role in Cybersecurity- The Basics



LOCK DOWN YOUR LOGIN



WHEN IN DOUBT, THROW IT OUT



KEEP A CLEAN MACHINE



BACK IT UP



OWN YOUR ONLINE PRESENCE



SHARE WITH CARE



GET SAVVY ABOUT WIFI HOTSPOTS

**CYBERSECURITY IS
EVERYONE'S JOB.**

INCLUDING YOURS.



**CYBERSECURITY
AWARENESS
MONTH**

[STAYSAFEONLINE.ORG/](https://staysafeonline.org/)
CYBERSECURITY-AWARENESS-MONTH



Do Your Part. #BeCyberSmart



Beyond the Basics: Misinformation, Disinformation, Hoaxes, and Scams

Laundry List of Browser Plug-Ins and Sites Focused on Disinformation

<https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html>

The screenshot shows the homepage of the Global Disinformation Index (GDI). At the top left is the GDI logo with the text "Global Disinformation Index". To the right are navigation links: "RESEARCH", "THE INDEX", "ABOUT", and "NEWS". Below the navigation is a red headline: "Time to defund the coronavirus infodemic. Read how". The main content area has a dark blue background with a network diagram. The title "GLOBAL DISINFORMATION INDEX" is centered, followed by the subtitle "Disrupting the business model of disinformation". Below this are three dark blue boxes: "RESEARCH" (From adtech to adversarial narratives, GDI explores the most urgent issues in disinformation. Read our in-depth reports), "THE INDEX" (We provide a non-partisan, trusted and independent rating of disinformation risks for news sites. Read our methodology), and "LATEST" (Want to know about the coronavirus and more? See what is happening with GDI in the media? Read the latest news section). At the bottom of the main area is the text "WHY NOW?".

Do Your Part. #BeCyberSmart

Beyond the Basics: Misinformation, Disinformation and Hoaxes Example



https://disinformationindex.org/wp-content/uploads/2020/10/GDI_Ad-deck_-US_Primer.pdf

GDI has studied a selection of popular brand ads appearing on US election disinformation on the five top traffic sites carrying this content

Conspiracy theories include:

- Political parties are actively buying votes.
- Party-linked groups planning electoral violence.
- Parties are actively disrupting mail-in ballot processes.
- Candidates are calling for violence.
- Candidates are unfit and too old to hold office.

GDI

These conspiracies form part of a broader disinformation landscape around the US elections.

These narratives are being framed around or within stories.

GDI

Figure 1: Election Disinformation Map

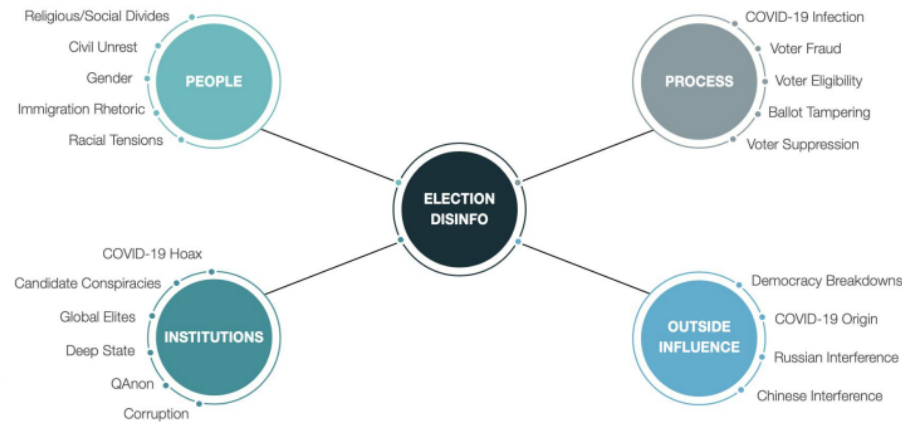


Figure produced by the Global Disinformation Index

Sample of popular brands funding these stories:



Do Your Part. #BeCyberSmart

Beyond the Basics: Scams



Example of Phishing Scams at SF State

From: Corey Roberts <corey@districtadvice.com>
Sent: Tuesday, October 20, 2020 10:56 PM
To:
Subject: Retirement Support for San Francisco State University Personnel

Employee <LAST NAME>,

Each year, as an employee of San Francisco State University you are eligible to schedule a phone call, teleconference, or in-person meeting off campus with a representative for answers to your specific state, federal and individual retirement benefit questions.

At your consultation, you will be provided with information that will tell you what your potential income can be when you retire, and how much longer you may have to work. That, along with advice on the best ways to utilize your 401(a)/403(b) options with your state retirement and/or Social Security benefits.

Please be sure to indicate which type of appointment you prefer (off-campus, phone call, or teleconference) in the notes section while scheduling. Please also include your direct cell phone number.

Appointments fill up quickly. If you'd like to secure your spot, click on the link below, or simply reply "yes" to this email.

<https://districtadvice.com/index.html#appointment/4f63f171-ec77-4eec-a79f-da3c73e68df7>

Licensed representatives are not employees of the college or state retirement system. All representatives are independent and licensed by the state department of insurance.

To opt out of future mailings, click on the following link:

<https://districtadvice.com/index.html#appointment/4f63f171-ec77-4eec-a79f-da3c73e68df7/unsubscribe>



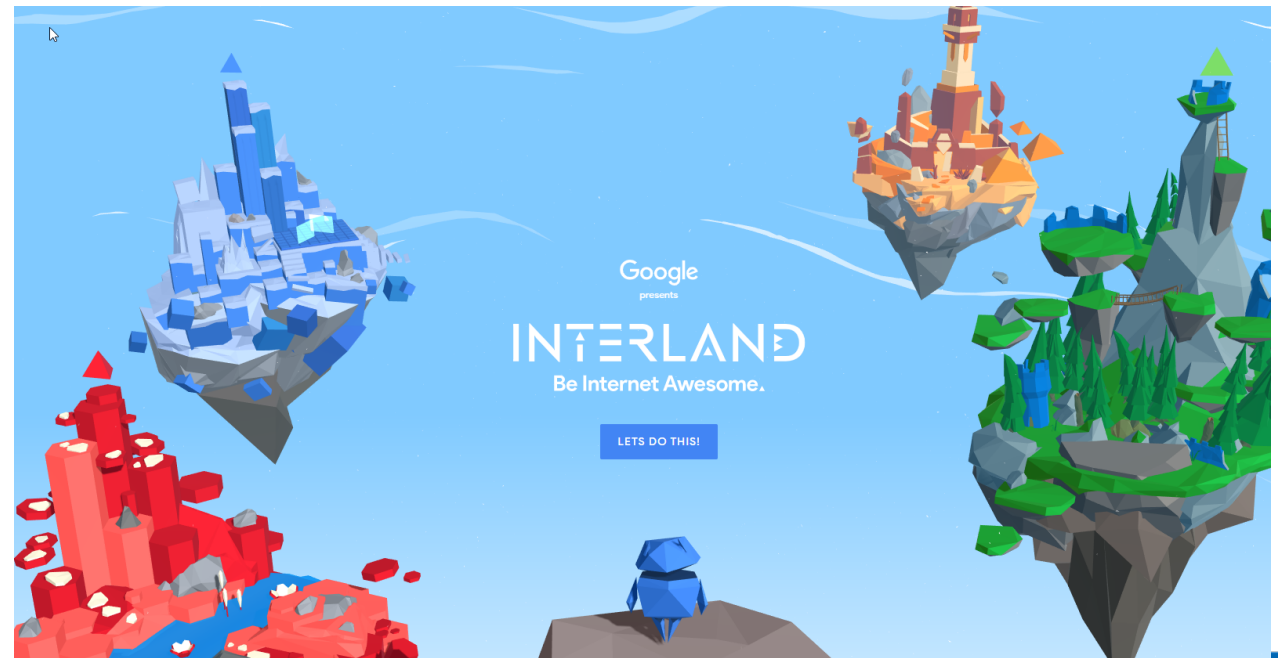
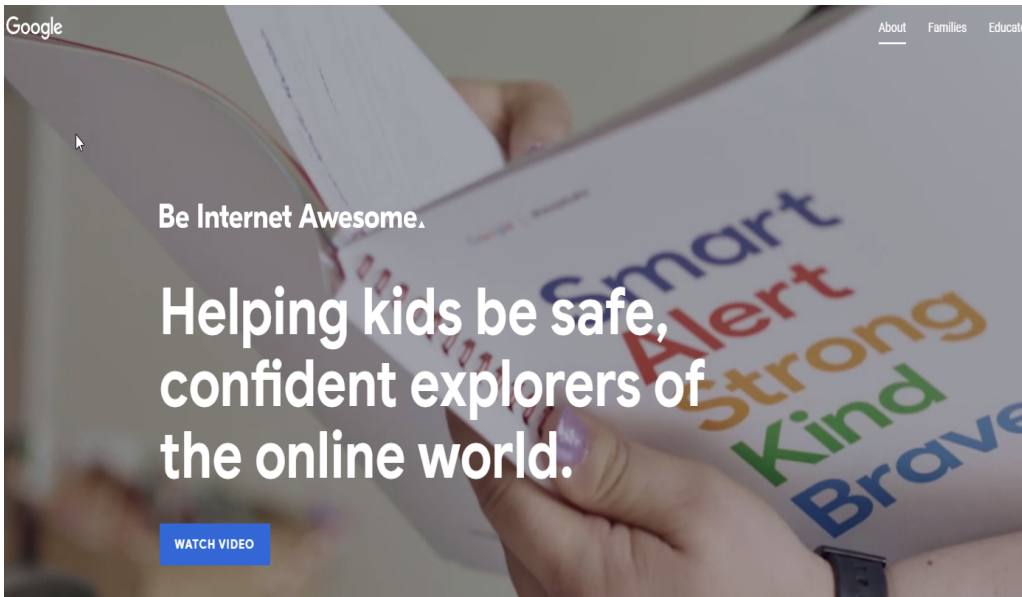
Do Your Part. #BeCyberSmart

Educate Yourself and Your Family



Be Internet Awesome: https://beinternetawesome.withgoogle.com/en_us

Game: https://beinternetawesome.withgoogle.com/en_us/interland



Do Your Part. #BeCyberSmart



Mobile Devices

Top Security Best Practices

- ❖ Keep software up to date
- ❖ Password protect your device
- ❖ Use security software (e.g. Lookout Personal, BitDefender Mobile)
- ❖ Set up the Locate/Find Me Feature

Top Privacy Best Practices

- ❖ Know when you have geo-location turned on
- ❖ Review privacy settings and the access needed when downloading mobile apps
- ❖ Don't store personal or confidential information on a mobile device





Internet of Things (IoT) Devices

Pros	Cons
Convenient	Vendors may not be able to push out fixes for vulnerabilities
Easy to use and set up	User doesn't have complete control of the device
Fairly low cost	Could be susceptible to hostile take-over or data leaking
Connect and control with smart phones	Has ability to impact real-world (people, things)

Think through all considerations when making decisions about using IOT devices.

Examples: NEST Thermostats, home surveillance cameras, Purple Air - Air Quality Sensors, TV's, streaming devices, smart garage door openers



Other Considerations



- Dedicate a device for work/learning
 - Do not share the computer for other uses
 - Do not co-mingle work and personal data
- Ergonomics
 - Neutral positions for head/eyes, back and wrist (See SF State's Resources)
 - Eye Strain considerations
 - Try the 20-20-20 rule: Every 20 minutes, look at something 20 feet away for at least 20 seconds.



SF State Resources



SF State Cybersecurity Awareness Month:

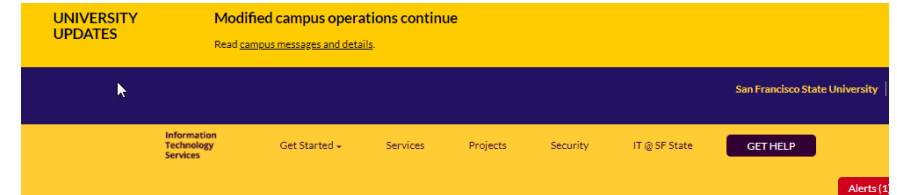
- <https://its.sfsu.edu/announcement/cybersecurityawarenessmonthoctober2020>

SF State Remote Work Resources:

- <https://its.sfsu.edu/guides/continuitytools>
- <https://dev-sfsu-at.pantheonsite.io/departamental-operations-continuity-resources>

SF State Ergonomics:

- <https://erm.sfsu.edu/content/ergonomics>
- <https://erm.sfsu.edu/sites/default/files/Setting%20Up%20Your%20Laptop%20In%20Your%20Home.pdf>
- <https://erm.sfsu.edu/sites/default/files/Ergonomic%20%20Tips%20for%20Using%20Laptops.pdf>
- <https://www.mayoclinic.org/diseases-conditions/eyestrain/diagnosis-treatment/drc-20372403>



2020 Cybersecurity Awareness Month



October is Cybersecurity Awareness month and the theme this year is:
Do Your Part - Be Cyber Smart!
Each week will focus on a different area to highlight the corresponding cyber security risks and tools/tips to reduce/mitigate them.

Weekly Content



Do Your Part. #BeCyberSmart

NCSA Resources

Cybersecurity Awareness Month:

<https://staysafeonline.org/cybersecurity-awareness-month/>

COVID-19 Security Resource Library:

<https://staysafeonline.org/covid-19-security-resource-library/>

Security Awareness Videos:

<https://staysafeonline.org/resource/security-awareness-episodes/>



OWN YOUR ROLE IN CYBERSECURITY: START WITH THE BASICS

Every individual should own their role in protecting their information and securing their systems and devices. There are many steps individuals can take to enhance their cybersecurity without requiring a significant investment or the help of an information security professional.

Below, NCSA highlights eight tips you can put into action now:

CYBERSECURITY BASICS:



MAKE A LONG, UNIQUE PASSPHRASE

Length trumps complexity. A strong passphrase is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember.



PASSPHRASES AREN'T ENOUGH

Use 2-factor authentication or multi-factor authentication (like biometrics, security keys or a unique, one-time code through an app on your mobile device) whenever offered.



WHEN IN DOUBT, THROW IT OUT

Links in email, tweets, texts, posts, social media messages and online advertising are the easiest way for cyber criminals to get your sensitive information. Be wary of clicking on links or downloading anything that comes from a stranger or that you were not expecting. Essentially, just don't trust links.



KEEP A CLEAN MACHINE

Keep all software on internet connected devices – including personal computers and tablets – current to reduce risk of infection from ransomware and malware. Devices to automatically update or to notify you when an update is available.

staysafeonline STAYSAFEONLINE.ORG



Looking for a new job can be a daunting project, and frequently involves the exchange of personal information with complete strangers—which is why job seekers are an enticing target for cyber criminals. As you look for a new job, be extra vigilant so your application materials and personal information don't end up in the wrong hands.

TIPS TO PROTECT YOURSELF

DO YOUR RESEARCH

- Conduct a web search of the hiring company using the company name only. Results that return multiple websites for the same company (abccompany.com and abccompany1.com) may indicate fraudulent job listings.
- Check for spoofed websites. Scammers will often spoof legitimate websites with the exception of small discrepancies in order to deceive victims.
- If the hiring company is well known and has a website, contact the company to confirm the legitimacy of the job listing. It is likely the legit company has received other calls and can confirm a scam listing.

DON'T PAY TO PLAY

- Never send money to someone you meet online, especially by wire transfer, prepaid cards, or money transfer apps.
- If you receive any paper checks with instructions to purchase items or transfer money, contact the financial institution on the check to ensure the availability of funds.
- Never provide credit card information to an employer.
- Never provide bank account information to employers without verifying their identity.

PAUSE BEFORE SUPPLYING SENSITIVE INFO

- Legitimate companies will ask for personally identifiable information (PII), such as social security number and bank account information for payroll purposes, AFTER hiring employees.
- Before entering PII online, make sure the website is secure by looking at the address bar. The address should begin with "https://", not "http://".
- However, criminals can also use https:// to give victims a false sense of security. A decision to proceed should not be based solely upon the use of "https://".

staysafeonline Facebook.com/staysafeonline FBI facebook.com/FBI
WWW.STAYSAFEONLINE.ORG WWW.FBI.GOV

Access tip sheets, videos, infographics and more at

<https://staysafeonline.org/resources/>

Do Your Part. #BeCyberSmart

CISA Resources



STOP. THINK. CONNECT.™

<https://www.cisa.gov/stopthinkconnect>

#BeCyberSmart Campaign

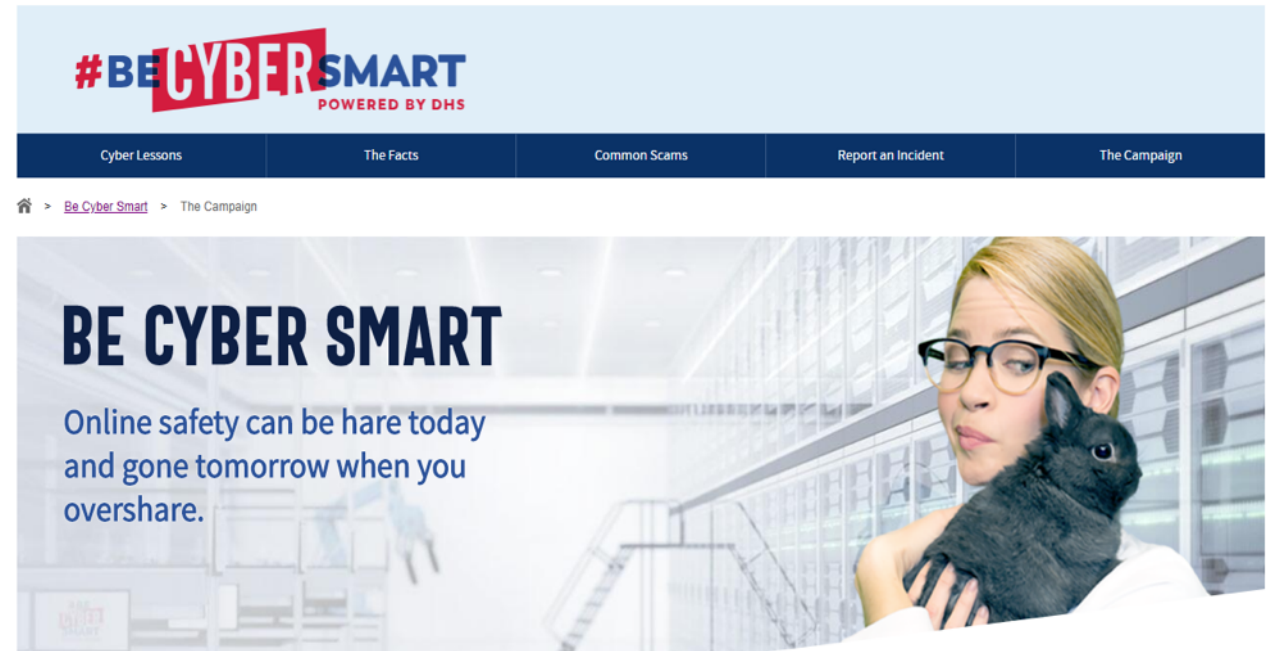
<https://www.dhs.gov/be-cyber-smart/campaign>

CISA's Cyber Essentials

<https://www.cisa.gov/cyber-essentials>

Telework Guidance & Resources

<https://www.cisa.gov/telework>



Do Your Part. #BeCyberSmart



SF STATE

Keep In Touch

Twitter:
[@SFSU_ITS](https://twitter.com/SFSU_ITS)

LinkedIn:
[Information Technology Services](https://www.linkedin.com/company/information-technology-services)

Email:
service@sfsu.edu



ITS @ SFSU
1,625 Tweets

ITS @ SFSU
@SFSU_ITS

Providing reliable and secure enterprise-wide apps and infrastructure to support SFSU's long-standing commitments to teaching, learning, and social justice.

San Francisco, CA its.sfsu.edu Joined September 2017

252 Following 165 Followers

Tweets Tweets & replies Media Likes

ITS @ SFSU @SFSU_ITS · 6h
Want to learn more about protecting yourself and your family from online threats? Register for a Cybersecurity Awareness Month presentation to be held 4 p.m. Wednesday, Oct. 21, via Zoom. Registration at its.sfsu.edu/content/events...

ITS @ SFSU @SFSU_ITS · 21h
No matter how long and strong your passphrase is, a breach is always possible. Make it harder for cyber criminals to access your account by enabling multi-factor authentication. Lock down your login! [#BeCyberSmart](#)

OCTOBER IS