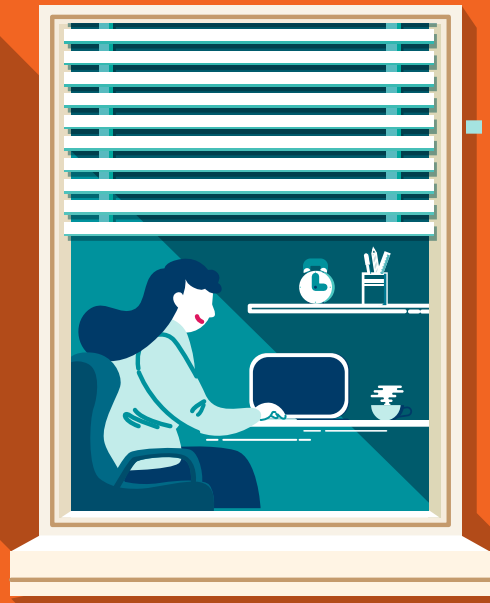


Stanislaus Community Online Safety



STAY HOME



STOP COVID-19

- Beware of social engineering and phishing tactics in emails, phone calls, or text message.
- Do not click on links or attachments to emails or texts from unknown senders.
- Do not provide the password, birth date, Social Security number, financial data, or personal information in response to an email, text, or phone call.
- Hackers may disrupt video teleconferencing by inserting inappropriate images and threatening language if the meeting is not set-up correctly.
- Be aware of advertisements or emails purporting to be from legitimate sources. Always verify the web address to make sure it is from a safe source.
- Be wary of social media promotions.
- Secure your Wi-Fi at home. Change the default password immediately. Call your Internet Provider for assistance.
- Create strong passwords for online accounts. If you bank online, use multi-factor authentication (MFA) when accessing your account. Contact your bank for assistance.
- Make sure your devices have anti-virus software installed, and updates are applied regularly.
- Backup your computer regularly.