October 2022

Wellness and Safety Bulletin – Cybercrime Prevention

California Department of Developmental Services

Is this bulletin useful?

Click here.

Cybercrime Prevention

The internet is a great way to connect on-line, but it can also be dangerous. Just like when you prepare to leave your house, you should take precautions before using the internet to make sure you and your information are safe and secure so that you do not become a victim of cybercrime.

How to Stay Safe on the Internet

What is Cybercrime?

Cybercrimes are crimes that happen to people over the internet. They occur when someone's personal information or their money is stolen. Many people do not know when a cybercrime is happening to them, so it is important to know how to recognize cybercrimes to prevent it or to get help and stop them from happening again.

The Internet is a Public Space

- People can see what website you are going to and, sometimes, what information you type in.
- Any information you share on the internet may be seen by someone else.
- Be very careful about sharing your personal information (like social security numbers, bank account information, and medical information) on the internet when it is not for a valid business reason, like banking.
- Public Wi-Fi networks at stores and restaurants that are allow you to use it for free should always be used with caution.
- Although using public Wi-Fi is convenient, it often lacks security. This means that your personal information (like the username and password to your bank account, for example), may be seen or stolen by other people.

Check Privacy Settings Regularly

- Privacy settings allow you to choose what information you want to share and who sees your information.
    - On social media (like Facebook or Instagram), you can use privacy settings to control what information is shared with others.
- Set privacy settings for different applications on your cellphone to limit what gets shared with the applications (like share your location or data permissions).
- Make sure that the privacy settings on your online accounts require a password before accessing your accounts.
    - Two Factor Authentication is when you receive a text, call, or email with a special code every time you log in to your online account (like the bank or credit card company). This helps to make sure it is really you logging into your account.
    - It is a good idea to set up Two Factor Authentication for online accounts.

Use Strong Passwords for Online Accounts

- Make your password strong and remember to change it regularly. This will protect your online accounts.
- A strong password has at least 8 characters, and includes a combination of upper and lowercase letters, symbols, and numbers. The longer the password, the safer it is.
    - **Examples of weak passwords**: password, YourName, 12345
    - **Examples of secure passwords**: 8blu3Car$dr1vinG, 1&n%00Xb#, Y3!!oWfL0w3rs
- Avoid passwords that are easy to guess, like your birthdate or name.
- Each of your accounts should have its own unique password.
- Don't keep a list of passwords on a sheet of paper laying around, especially near your computer.
- Passwords should only be shared with people that you know and trust and should be kept in a safe place.

Watch for Viruses and Malware

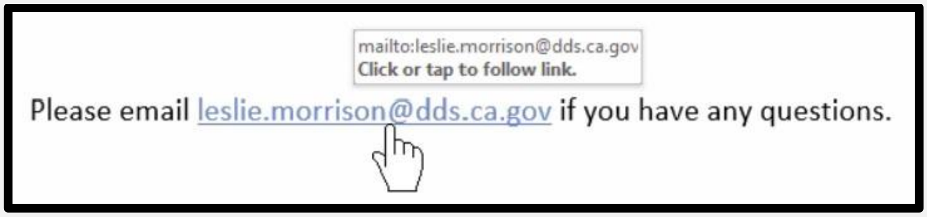
- ***Malware*** is a type of software that is harmful to your computer. ***Viruses*** are a type of malware.
    - Viruses and malware enter a computer system without your permission and "infect" it.
    - Viruses and malware can steal your information, slow down and crash your computer, or take complete control of your computer.
- Viruses and malware get into your computer when you click a link or open an email that is infected with them.
    - Be careful before clicking on a link that offers you a prize or something for free.
    - These can look like games, screen savers, or downloads but can be malware or viruses.

Think Before you Click

- Pay attention to the senders of emails and messages you receive online.
    - Check their email address to see if it matches with the address you already have for them.
- Be especially careful if the sender is rushing you to answer right away or makes it seem like there is a crisis, such as a problem with your bank account. These types of messages are most likely a scam.
- Phishing is an internet scam that tricks people into sharing their personal information by using fake messages that look real.
    - Before replying to the messages, check for an unfamiliar sender, spelling or grammar mistakes, links that don't match the content of the message, random attachments, and a request for you to act fast.
- Don't open attachments or click on links that you don't recognize. These could be fake and lead to viruses being installed that can harm your computer or phone or steal more information from you.
    - When you receive an unexpected email with links or attachments always check with the sender (by phone or text) to make sure it was them that sent it.
- The IRS will only send you notices in the U.S. mail. Do not respond to calls, emails or text messages that say they are from the IRS.

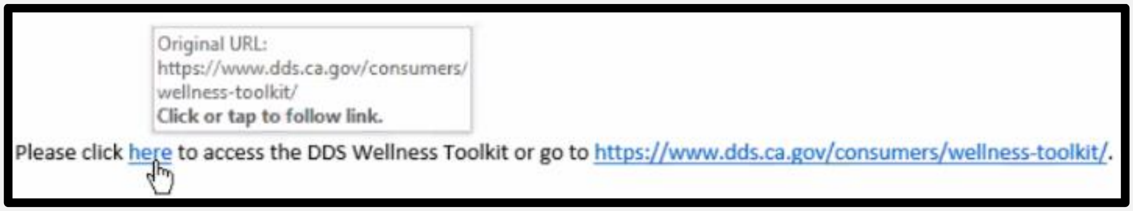
Know who you are Emailing or Texting

- Remember that people online may not be who they say they are.
- Never share personal information or send photos of yourself to a stranger or someone that you have never met in person.
- Never send money to someone that you have only recently met or have never met in person.
- Before you enter your social security number or any account numbers into an online form or website, make sure the sender asking for the information is really who they say they are.
    - Check the email address of the sender by moving the cursor over their name or the link to make sure it looks like it is going to the right business.



mailto:leslie.morrison@dds.ca.gov
Click or tap to follow link.

Please email leslie.morrison@dds.ca.gov if you have any questions.



Original URL:
https://www.dds.ca.gov/consumers/wellness-toolkit/
Click or tap to follow link.

Please click here to access the DDS Wellness Toolkit or go to https://www.dds.ca.gov/consumers/wellness-toolkit/.

- People can copy logos and make emails look and sound real, so look at them carefully for misspellings, odd content or fuzzy images.
- If you are not sure the sender is real, contact the company or organization from your online account or call them directly.

What to do if You Have Been the Victim of Cybercrime

- Tell someone you trust right away.
- If the crime involved accessing your personal accounts, call your bank or credit card company and let them know right way. Stop using any of the debit or credit cards for accounts that have been accessed.
- Change your password to any account or login that has been attacked.
- Watch your accounts for unusual activity.

Wellness and Safety Bulletins are produced by the Department of Developmental Services to alert individuals, families, and others to specific risks identified with our community.
Please provide feedback on this bulletin and what we can do better through this survey: Bulletin Survey