Cybercrime Prevention

Cybercrime is a serious and growing issue for internet users. Although staying connected online is great, there are things to know about safely using the internet. Cyber criminals target people they believe are vulnerable, including people with Intellectual and/or Developmental Disabilities. Everyone should be aware of the risks of cybercrime and how to stay safe while browsing the internet.

What is Cybercrime?

Cybercrimes are crimes committed over the internet using mobile devices (like cellphones), computers, and public internet Wi-Fi networks. Cyber criminals steal sensitive or personal information for financial profit.

Individuals are targeted through a variety of strategies to covertly gather personal information. Many people unknowingly fall for cybercrimes which often result in financial loss (theft), personal data breaches, and identity theft for the victim. Knowing how to prevent and seek help following cybercrimes is more important than ever before.

Cyber criminals are opportunistic and seek vulnerable populations to prey upon. With individuals with IDD, criminals may know their victim or endear themselves an acquaintance or trustworthy person.

Common Types of Cybercrime

Phishing: Using email, text messages, and telephone calls to get victims to reveal personal or financial information, and/or login credentials.

Non-Delivery: Using the internet to illegally solicit electronic payment for the purchase of goods and services that are never received.

Extortion: Getting money or goods through intimidation or threats from someone posing to be from an authority (like the IRS). It may include threats of physical harm, criminal prosecution, or public exposure. It could also involve locking access to the victim's data and holding it for ransom.

Personal Data Breach: Stealing and sharing an individual's private personal information and data to an unauthorized user.

Identity Theft: Stealing and using another individual's personal information to commit fraud or other crimes.

Cybercrime in the U.S. In 2020

- During the COVID pandemic, individuals with IDD were the victim of cyber criminals who diverted federal stimulus money that was sent to them electronically.
- California had the highest number of cybercrime complaints in the nation.
- The FBI received almost 800,000 cybercrime complaints from the public, a **69% increase** from the previous year.
- Phishing was the most common cyberattack with over **241,000** reported victims.
- Reported losses exceeded **$4.1 billion**.
- Individuals over the age of 60 were the most victimized of any age group.

Help Protect the Individuals you Serve from Cybercrime

The internet is a public space

Remind individuals to be very careful before sharing personal information, like social security numbers, bank account information, and medical information on the internet.

- **Public Wi-Fi networks should always be used with caution.**
- Public Wi-Fi networks are open to anyone if they are within range, and do not usually require users to agree to any terms or conditions before joining.
- Although using public Wi-Fi is convenient, it often lacks security. This means that personal information (like username and passwords), can potentially be viewed electronically by other people without the victim knowing.
- Secured Wi-Fi networks often require a user password and may require a fee or purchase to use.

Use Strong Passwords for Online Accounts

Help the individuals you serve to create strong passwords.

- Encourage individuals to not use common passwords or passwords that can be easily guessed.
- 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.
  - **Weak passwords**: “password”, your name or birthday, 12345,
  - **Strong passwords**: 8blu3Car$dr1vinG, 1&n%00Xb#, Y3!!oWfL0w3rs

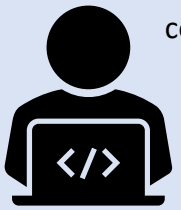
Check privacy settings regularly

Help individuals you serve check privacy settings on their mobile devices and computers. Explain how to set up Two Factor Authentication by adjusting privacy settings on the online accounts. Two Factor Authentication is when the user is sent a text or email with a special code every time the individual logs onto their online account.

Wellness and Safety Bulletins are produced by the Department of Developmental Services to alert direct service providers, regional centers, 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

Viruses and Malware

- ***Malware*** is a type of software that is designed to harm a mobile device or computer system.



  - ***Viruses*** are computer codes that enter a computer system without permission and "infect" it. They hide in files or applications sent by email or text and infect a computer when they are opened. Viruses are a type of malware.
- Viruses can steal user information, slow down and crash the computer, or take complete control of a computer or device.
- Viruses cannot spread on their own. They spread when people unknowingly share them. This commonly occurs through sharing infected files or emails.

What to do After Being the Victim of Cybercrime

Explain the importance of calling their bank and cancelling their debit or credit cards used in the cyberattack. Help with changing login information for online accounts. Alert the institution of account that was hacked about the attack and inquiring about any fraudulent charges credited.

The DDS Wellness Toolkit has more information about how to help support and protect the individuals you serve.

Helpful Resources

Local Law Enforcement

Internet Crime Complaint Center (IC3)

Federal Trade Commission (FTC)

- Report fraud at ReportFraud.ftc.gov
- Call the FTC hotline at 1-877-IDTHEFT (1-877-438-4338)
- Report identity theft and find more information at identitytheft.gov

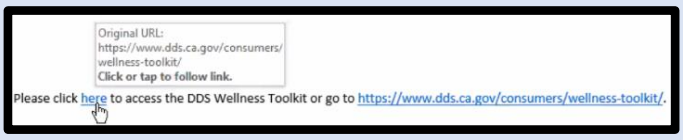
Think Before you Click

- Discourage the individuals you serve from opening unsolicited attachments or clicking on unrecognizable links. These could lead to viruses or malware that can harm computers.
- Warn individuals to be cautious before clicking on links that look like games or that promise getting something "free" if they click the link.
- Encourage individuals to check the address of emails they receive to confirm that the sender is legitimate. If they receive an unexpected email with links or attachments, suggest they contact the sender by phone or text to confirm that they sent the email.
- Phishing is a common internet scam that tricks people into sharing their personal information through the use of fake messages that look real.
  - Before responding to any messages, be aware telltale signs of a phishing scam: an unfamiliar sender, spelling and grammar mistakes, suspicious links that don't match the content of the message, random attachments, email content that with a sense of urgency.

Before Replying to or Clicking on an Email

Encourage consumers to verify who is sending them emails.

- 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.



Wellness and Safety Bulletins are produced by the Department of Developmental Services to alert direct service providers, regional centers, 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