LEAVING your DIGITAL FOOTPRINT

Attorney General Jeff Landry
Louisiana Department of Justice

> You do a lot on your phone. You text, email, and share photos and videos. You update your status, post comments, and send direct messages on social media.

Social networking sites and apps have exploded in popularity in recent years. While they can be helpful in connecting with friends, these online platforms are also prime targets for criminals.

Recent studies show that 1 in 9 young adults have experienced unwanted sexual requests online and that 1 in 5 have been exposed to unwanted sexual content online.

What's more: researchers have also found that technology platforms have "paved the way for the greater blurring of boundaries for the engagement of bullying across settings such as school, home, and cyberspaces."

To combat these dangers, my office has compiled this brochure to help you protect your digital footprint and ensure your privacy online.

If you have questions or would like more information, please visit www.AGJeffLandry.com/CyberSafety.

WHAT IS A DIGITAL FOOTPRINT?

Your digital footprint is the trail you leave behind when you post information about yourself online.

Passive Digital Footprint - Information that a user doesn't know is being tracked, such as cookies, IP addresses, and search history.

Active Digital Footprint - Information that a user intentionally places online, like emails sent, blogs published, and content posted on social media.

WHAT IS OVERSHARING?

Oversharing is when people share too much personal information with the public or a stranger. It can happen both online and offline. However, it is a big problem on social media, which makes "putting yourself online" easy.

EXAMPLES

- Using social media to vent your emotions
- Announcing vacation plans or other times when you will not be at home
- Posting lewd or inappropriate photos
- Sharing intimate details about your life
- Allowing apps or others to know your location

THE DANGERS OF OVERSHARING

When you're so heavily involved in social media that you're oversharing, it can lead to big problems like...

Security Issues - If people really want to stalk or target you in some way, they can learn about you by looking at your profile. The more info you share, the more they know.

Damages to Personal Reputation - If you click without thinking, it can have huge consequences. You never know who will see your posts, photos, or comments.

Missed Opportunities - Your online reputation affects everything, from school acceptance to job employment to even relationships with others.

SEXTING

Using your phone or another electronic device to send sexual pictures of yourself or others can get you into trouble with the law.

Nude pictures of juveniles under the age of 18 is illegal child sexual abuse imagery, and its production and distribution are very serious crimes.

People who ask for and transmit such graphic things can get arrested as child pornographers and sex offenders.

CYBERBULLYING

Cyberbullying is the use of technology to harass, embarrass, or target another person. Online bullying, like other kinds of bullying, can lead to serious long-lasting problems. Cyberbullying can include:

- Intimidation or online threats
- Aggressive or rude texts
- Posts of personal information to hurt or embarrass someone else
- Prank calls to someone's cell phone
- Hacks into someone's gaming or social networking profile
- Fake accounts spreading hurtful messages online

COMMON PLACES CYBERBULLYING OCCURS:

- Social media platforms, such as Facebook, Instagram, Snapchat, and Tik Tok
- Text messaging and messaging apps
- Video gaming communications
- Online forums and chat rooms

CYBERSTALKING

The United States Department of Justice defines stalking as conduct “directed at a specific person that would cause a reasonable person to fear for his or her safety or the safety of others or suffer substantial emotional distress.”

According to the Bureau of Justice Statistics, 1 in 4 stalking victims also reported cyberstalking through emails/instant messaging.

EXAMPLES

- Unsolicited contacting via phone calls, emails, or texts
- Following or watching a victim
- Posting information or spreading rumors about someone on the internet

WHAT DO I DO IF I AM BEING STALKED?

- If you are afraid that you are in immediate danger, do not hesitate to contact 911.
- Document every interaction.
- Contact the police to file a complaint and be sure to present them with evidence.
- End all contact. Do not respond to any further messages and block the cyberstalker.
- Disable location services and geotagging on your phone and photos.

LEGAL CONSEQUENCES

Cyberstalking (LA R.S. 14:40.3) In Louisiana, sending an e-mail or any other form of electronic communication threatening to commit bodily harm or physical injury to another person or their property for the purpose of extortion of money or any other thing of value is against the law. In addition, repeatedly sending E-mails or other forms of electronic communication for the purpose of threatening, terrifying, or harassing any other person is against the law in Louisiana. If found guilty one serves up to two years in prison and can be fined up to $5,000.

Cyberbullying (LA R.S. 14:40.7)
Any transmission of electronic, textual, visual, or oral communication with the intent to coerce, abuse, torment or intimidate a person under the age of 18 years is illegal in Louisiana. Committing the crime of cyberbullying in Louisiana can land you in jail for six months.

LEGAL CONSEQUENCES (CONT.)

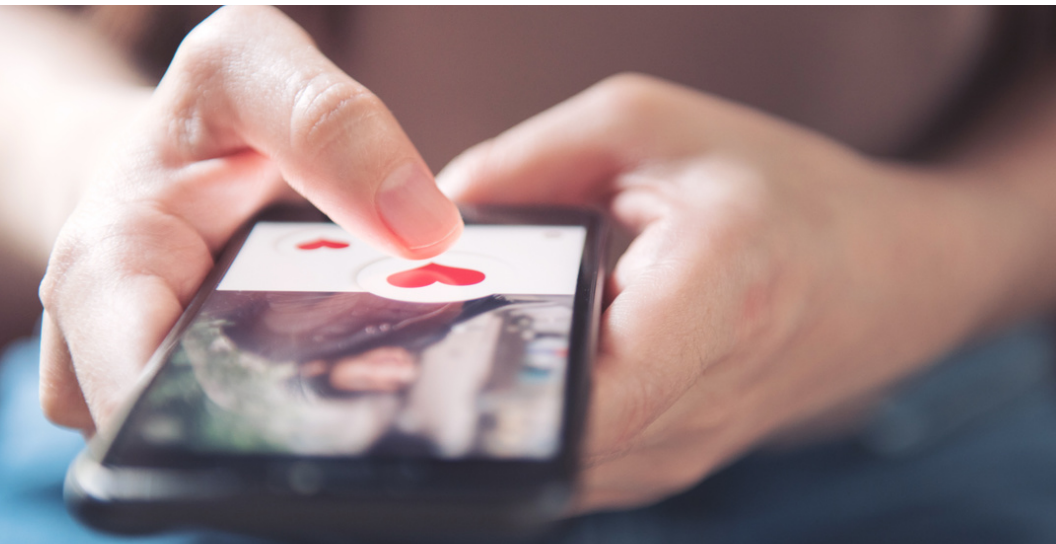
Sexting (LA R.S. 14:81.1.1) In Louisiana, it is unlawful for any person under the age of seventeen years of age to voluntarily use a computer or any Internet-accessible device to knowingly possess and/or transmit an indecent visual depiction of themselves or another person under the age of 17. If found guilty of sexting one can be fined up to $750 and imprisoned up to six months in prison or both.

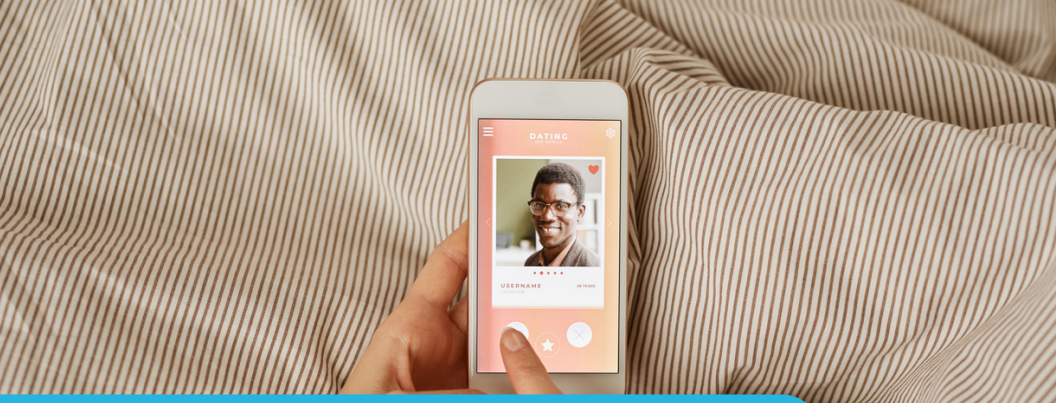
ONLINE DATING

Online dating has gone mainstream. Researchers have found that 40 million Americans use dating apps to find a relationship.

While many people find relationships through technology, it's not always a pleasant experience. In fact, online dating can be downright dangerous. Not everyone online is looking for love. Some people use the site to look for victims. Research shows:

- 10% of sex offenders use dating sites
- 1 in 10 users on free dating apps are scammers
- Sexual assault linked to online dating platforms have grown six-fold in the last five years





ONLINE DATING SAFETY TIPS

To help you safely embark on your quest for finding that “special someone," keep these tips in mind:

- Do a simple Internet search before meeting your date. Have at least some idea as to who the person is before you meet with him or her. If possible, try to find pictures and see what additional information comes up about the person beyond what is listed on the app or other social media platforms.

- Do not accept an invitation to carpool; take your own vehicle or use public transportation, if possible.

- Avoid going somewhere private with your date. Instead, meet at a public place where there are plenty of people around.

PHISHING

Some people use instant messages and emails to trick you into giving them personal information. Never respond to an email that is asking for your credit card information, address, or social security number.

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may...

- Say they've noticed some suspicious activity or log-in attempts;
- Claim there's a problem with your account or your payment information;
- Say you must confirm some personal information;
- Include a fake invoice;
- Want you to click on a link to make a payment; and/or
- Say you're eligible to register for a government refund.

MINIMIZING YOUR FOOTPRINT

Most people have created many accounts over time for gaming, online shopping, and socializing. These are easy to forget but important to manage.

- Try to access your old accounts, delete your personal information, and deactivate the accounts.

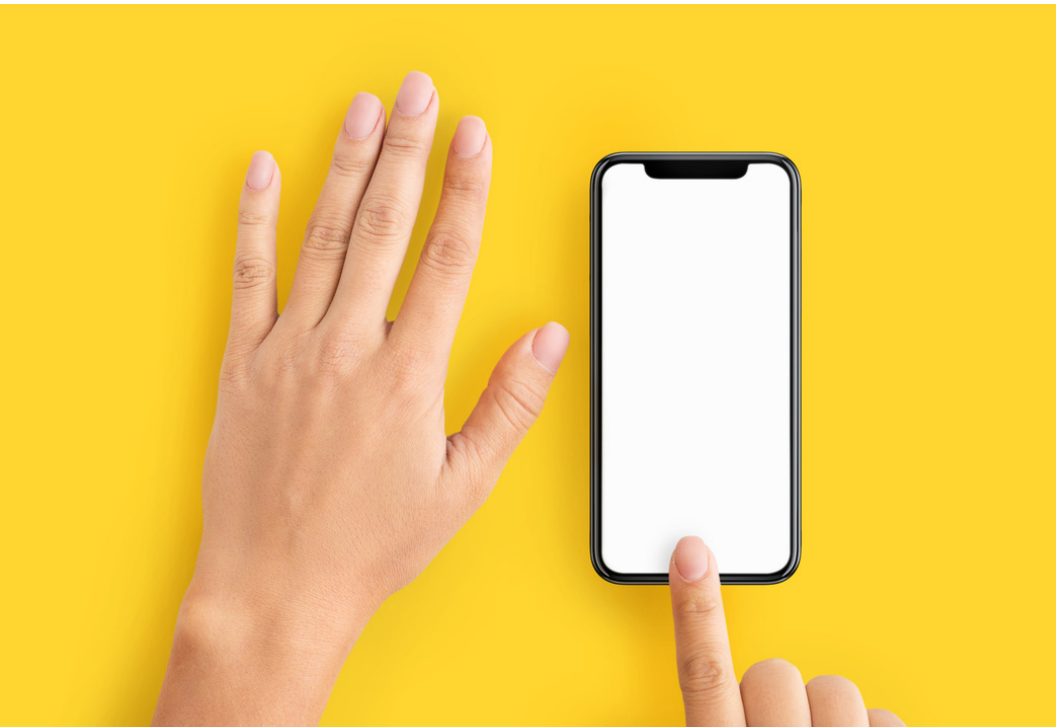
- Do a quick online search of yourself. If there are still photos or account details appearing that you're not happy with, then you may need to think about other options like creating new accounts in your name and sharing content publicly that better reflects who you are.

- Check your privacy settings and ask apps to not "track your location."

- Use "private browsing" within your web browser when surfing the web. This helps prevent your passwords, search records, and browsing history from being saved on that device.

MINIMIZING YOUR FOOTPRINT (CONT.)

- Don't click on surveys that ask for personal information.
- Use personal hotspots or secure Wi-Fi connections when accessing accounts that may contain personal information.
- If you’re going to post things like pictures and videos make sure there aren’t any notable landmarks or points visible. This will make it difficult for attackers to discover your whereabouts.



NOTES

This public document is published at a total cost of $3,261.66. Ten thousand (10,000) copies of this public document were published in this first printing at a cost of $3,261.66. This document was published by OTS-Production Support Services, 627 North 4th Street, Baton Rouge, LA 70802 to educate consumers about online dangers and provide helpful information on protecting citizens' digital footprints and privacy under the authority of LA R.S. 51:1404. This material was printed in accordance with standards for printing by State Agencies established in R.S. 43:31. Printing of this material was purchased in accordance with the provisions of Title 43 of the Louisiana Revised Statutes.