WHAT LGBTQ COMMUNITIES SHOULD KNOW ABOUT ONLINE SAFETY

One of the biggest concerns for LGBTQ individuals is the amount of information across multiple social platforms that could put their privacy at risk. As a result, your online conduct – from your interactions on social networks to the mobile apps you download – can lead to invasions of privacy and risks to safety. NCSA is happy to be partnering with LGBT Tech to provide tips and resources for staying safe online.

START WITH SECURITY BASICS

KEEP A CLEAN MACHINE
Keep all software on internet connected devices – including personal computers, smartphones and tablets – current to reduce risk of infection from ransomware and malware. Configure your devices to automatically update or to notify you when an update is available.

MAKE YOUR PASSPHRASE A SENTENCE
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 (for example, “I love eating sundaes on sundays.”). On many sites, you can even use spaces.

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 an easy way for cyber criminals to get to you. 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.

GET SAVVY ABOUT WIFI HOTSPOTS
Public wireless networks and hotspots are not secure, which means that anyone could potentially see what you are doing on your laptop or smartphone while you are connected to them. Limit what you do on public WiFi, and avoid logging in to key accounts like email and financial services. Consider using a virtual private network (VPN) or a personal/mobile hotspot if you need a more secure connection.
WHAT LGBTQ COMMUNITIES SHOULD KNOW ABOUT ONLINE SAFETY

PROTECT YOUR PERSONAL INFORMATION

KEEP PERSONAL INFO PERSONAL
Be cautious about how much personal information you provide on social networking sites. The more information you post, the easier it may be for a hacker or someone else to use that information to steal your identity, access your data, or commit other crimes such as stalking.

THINK BEFORE YOU ACT
Be wary of communications that push you for immediate action or ask for personal information. People online aren’t always as they appear. Online surveys are a great way for cyber criminals to collect personal information they can then use against you. For instance, don't trust online surveys that ask you to submit any personal information.

KNOW WHAT ACTION TO TAKE
If someone is harassing or threatening you, remove them from your friends list, block them and report them to the site administrator.

SHARE COMPUTERS WITHOUT SHARING INFORMATION
When using a shared computer in a community space, be sure to always log out of accounts and be mindful of your surroundings. You don't want others peering over your shoulder as you access your banking account. Did we mention to always log out of accounts when you're done? It’s worth mentioning again. Clicking “x” is not the same as clicking "logout".

REVIEW PRIVACY SETTINGS FOR ALL DEVICES AND ACCOUNTS
Every time you sign up for a new account, download a new app, or get a new device, immediately configure the privacy and security settings to your comfort level for information sharing. Regularly check these settings (at least once a year) to make sure they are still configured to your comfort.

DO AN ONLINE AUDIT
Perform routine Internet searches of your name and any words with which you wouldn't want to be associated. Find something you don’t like? Contact the website administrator immediately to have that content altered or removed.
WHAT LGBTQ COMMUNITIES SHOULD KNOW ABOUT ONLINE SAFETY

LEARN MORE

The National Cyber Security Alliance (NCSA) builds strong public/private partnerships to create and implement broad-reaching education and awareness efforts to empower users at home, work and school with the information they need to keep themselves, their organizations, their systems and their sensitive information safe and secure online and encourage a culture of cybersecurity. www.staysafeonline.org

LGBT (Lesbian, Gay, Bisexual, & Transgender) Tech encourages the continued early adoption and use of cutting-edge, new and emerging technologies by providing information, education and strategic outreach for LGBT communities. https://www.lgbtech.org/

PowerOn grants technology hardware to LGBTQ+ organizations across the country serving communities at the local level, ensuring connectivity for homeless, isolated, and disadvantaged LGBTQ+ individuals. The program empowers these people, giving them the tools to take charge of their circumstances and tackle the digital divide head-on. https://www.poweronlgbt.org/