Huntington Welcome.®

Help Keep Your Kids Safe Online

Today, families must think about safety and security both online and offline. Just like basic safety tips, such as not talking to strangers and looking both ways before crossing the street, teaching about online security is just as important as children spend more time on their devices both at home and at school.

Here are some important tips to help you get started:

☐ Create an open dialogue.

- Work together to set up rules for using digital devices, such as how long a child can be online, and appropriate websites and apps to visit.
- Ensure your children understand they can talk to you if they come across something that makes them feel uncomfortable.
- Have your children help you update software and privacy settings.
- Let your children teach you things about the Internet, computers and other technology.

☐ Always share with care.

- Help your children understand that any information they share online can easily be saved and is almost impossible to take back.
- Teach them to consider who might see a post and how it might be perceived in the future. Once something is online, it can be there forever.
- Just like the Golden Rule, teach your children to post about others as they would have others post about them.

☐ Personal information has value just like money.

- Information about your children, such as the games they like and their online searches, has value - just like money. Teach your children to be selective with the information they give to apps and websites.
- Teach your children to never tell strangers online their age, address, school name, where they hang out, or where they're going to be.
- Schools are required to send parents information about how they handle student privacy. Find out what information your child's school collects, how it's stored, who gets to see it, and what future administrators are allowed to do with it. Under the Family Educational Rights and Privacy Act (FERPA), you have the right to request, correct, or add an amendment to your child's records.

☐ Be empowered about your family's online presence.

- For children, utilize strict privacy settings in apps and on websites. Follow the instructions during initial set up, or go to "privacy" or "settings." Opt out of location sharing and the ability for the app or website to post or tag on social media sites on the child's behalf.
- Learn about and teach your children how to use privacy and security settings on their favorite online games, apps and platforms.
- Encourage your children to read the fine print before checking a box or entering an email address (or discourage them from giving out their email address all together).

92%

of teens surveyed go online daily with 24% using the internet "almost constantly"[1]

75%

of 13-17 year olds surveyed have at least one profile on a social media site[2]

Surveyed parents reported that

42%

of their children aged 8 and younger have their own tablet device[3]

[1] Source: "Teens, Social Media & Technology Overview 2015." Pew Research Center, Washington, D.C. (April 09, 2015) www.pewinternet.org/2015/04/09/teens-social-media-technology-2015.

[2] Source: American Academy of Child & Adolescent Psychiatry, *Social Media and Teens*

[3] Source: Common Sense Media, *The Common Sense Census: Media Use by Kids Age Zero to Eight 2017*

Turn over for additional tips.

☐ If it sounds too good to be true, it probably is.

- Teach your children to be skeptical of online offers that promise too much. Children and teens can be especially vulnerable to online scams, like those that promise a prize or free access to online games or apps, in return for personal information, such as emails, passwords or a parent's credit card.
- Also, fraudsters may try to trick your child into downloading malware through the premise of a free prize, app or game. Malware can perform harmful actions on your computer or other device that can steal personal information or cause performance issues.

☐ Remain engaged.

- Know the apps, social networks and websites your children use. Help them to identify safe and trusted websites and apps. Encourage them to be cautious about clicking on, downloading, posting and uploading content.
- Periodically check your child's social media network, texts and browser history from their devices. Make surprise checks, and having a parent as a 'friend' on social media, part of the agreement to have a device.

☐ Stay current.

- Keep up with new technology and ways to manage privacy.
- Use age-appropriate content controls.
- Keep antivirus software up-to-date to help guard against malware. Use parental controls, when available, to set guidelines for your children's online activities.
- Keep software updated.
- Protect all devices with passcodes that you and your child both know and change them at least three times a year.

Contact Huntington

If you receive a suspicious email, call or text claiming to be from Huntington, or think your account data has been compromised, let us know. We'll work with you to determine the legitimacy of suspicious messages and account activity.

PHONE: **(800) 480-2265**
EMAIL: **ReportFraud@huntington.com**

For more information about your privacy and security, go to **huntington.com/Privacy-Security**