CISA
CYBER+INFRASTRUCTURE

From: US-CERT * <US-CERT@ncas.us-cert.gov> The U.S. Computer Emergency Readiness Team
Subject: FBI Safe Online Surfing Challenge
Date: September 9, 2019 at 12:20:15 PM EDT
To: ewrussell3@icloud.com (Edmund W. Russell, III)
Reply-To: US-CERT@ncas.us-cert.gov

National Cyber Awareness System:

FBI Safe Online Surfing Challenge

09/09/2019 10:25 AM EDT
Original release date: September 9, 2019

The Federal Bureau of Investigation (FBI) has launched the Safe Online Surfing (SOS) Challenge, encouraging educators to promote web literacy and safety for students during the 2019-20 school year. FBI developed the program to educate children on how to navigate the web securely using activities that correspond with specific grade levels. Public, private, and home schools with at least five students are eligible to participate in the online challenge.
The Cybersecurity and Infrastructure Security Agency (CISA) encourages users to review the FBI SOS Challenge Announcement and
the **CISA Tip** Keeping Children Safe Online**.**
This product is provided subject to this Notification and this Privacy & Use policy.

Security Tip (ST05-002)

Keeping Children Safe Online

What unique risks are associated with children?
When a child is using your computer, normal safeguards and security practices may not be sufficient. Children present additional challenges because of their natural characteristics: innocence, curiosity, desire for independence, and fear of punishment. You need to consider these characteristics when determining how to protect your data and the child.

You may think that because the child is only playing a game, or researching a term paper, or typing a homework assignment, they can't cause any harm. But what if, when saving their paper, the child deletes a necessary program file? Or what if they unintentionally visit a malicious web page that infects your computer with a virus? These are just two possible scenarios.

Mistakes happen, but children may not realize what they've done or may not tell you what happened because they're afraid of getting punished.

Online predators present another significant threat, particularly to children. Because the nature of the internet is so anonymous, it is easy for people to misrepresent themselves and manipulate or trick other users (see Avoiding Social Engineering and Phishing Attacks for some examples). Adults often fall victim to these ploys, and children, who are usually much more open and trusting, are even easier targets. Another growing problem is cyberbullying. These threats are even greater if a child has access to email or instant messaging programs, visits chat rooms, and/or uses social networking sites.

What can you do?

- Be involved - Consider activities you can work on together, whether it be playing a game, researching a topic you had been talking about (e.g., family vacation spots, a particular hobby, a historical figure), or putting together a family newsletter. This will allow you to supervise your child's online activities while teaching them good computer habits.

- Keep your computer in an open area - If your computer is in a high-traffic area, you will be able to easily monitor the computer activity. Not only does this accessibility deter children from doing something they know they're not allowed to do, it also gives you the opportunity to intervene if you notice a behavior that could have negative consequences.

- Set rules and warn about dangers - Make sure your child knows the boundaries of what they are allowed to do on the computer. These boundaries should be appropriate for the child's age, knowledge, and maturity, but they may include rules about how long they are allowed to be on the computer, what sites they are allowed to visit, what software programs they can use, and what tasks or activities they are allowed to do.

- You should also talk to children about the dangers of the internet so that they recognize suspicious behavior or activity. Discuss the risks of sharing certain types of information (e.g., that they're home alone) and the benefits to only communicating and sharing information with people they know (see Using Instant Messaging and Chat Rooms Safely, Staying Safe on Social Network Sites, and the document Socializing Securely: Using Social Networking Services for more information). The goal isn't to scare them, it's to make them more aware. Make sure to include the topic of cyberbullying in these discussions (see Dealing with Cyberbullies for more information).

- Monitor computer activity - Be aware of what your child is doing on the computer, including which websites they are visiting. If they are using email, instant messaging, or chat rooms, try to get a sense of who they are corresponding with and whether they actually know them.
- Keep lines of communication open - Let your child know that they can approach you with any questions or concerns about behaviors or problems they may have encountered on the computer.

- Consider partitioning your computer into separate accounts - Most operating systems give you the option of creating a different user account for each user. If you're worried that your child may accidentally access, modify, and/or delete your files, you can give them a separate account and decrease the amount of access and number of privileges they have.

- If you don't have separate accounts, you need to be especially careful about your security settings. In addition to limiting functionality within your browser (see Evaluating Your Web Browser's Security Settings for more information), avoid letting your browser remember passwords and other personal information (see Browsing Safely: Understanding Active Content and Cookies). Also, it is always important to keep your virus definitions up to date (see Understanding Anti-Virus Software).

- Consider implementing parental controls - You may be able to set some parental controls within your browser. For example, Internet Explorer allows you to restrict or allow certain websites to be viewed on your computer, and you can protect these settings with a password. To find those options, click Tools on your menu bar, select Internet Options, choose the Content tab, and click the Enable... button under Content Advisor.

- There are other resources you can use to control and/or monitor your child's online activity. Some ISPs offer services designed to protect children online. Contact your ISP to see if any of these services are available. There are also special software programs you can install on your computer. Different programs offer different features and capabilities, so you can find one that best suits your needs.

***U.S. CERT**

(U.S. CERT) was developed in 2003 to protect the country's internet infrastructure and continues to play a vital role in keeping the public sector's data secured 24 hours a day, seven days a week. Working in collaboration with the Department of Homeland Security (DHS) and other private and public sectors, they strive to make the Internet safe for the entire nation. **REF: https://www.us-cert.gov/ncas/current-activity/2019/09/09/fbi-safe-online-surfing-challenge**

A copy of this publication is available at www.us-cert.gov. If you need help or have questions, please send an email to info@us-cert.gov. Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.