GKIS
GetKidsInternetSafe

CONNECTED FAMILY SCREEN AGREEMENT
CYBERSECURITY

GKIS Cybersecurity Introduction

“Unfortunately, cybercriminals can steal our online data just like a robber can steal money and jewelry. That means we have to follow special safeguards to assure our family’s cybersecurity, both at home and outside the home.”

“The goal of this part of our agreement is to make sure we all agree to follow basic cybersecurity practices.”

🔐 Cybersecurity

Cybersecurity setup:

☐ **We will protect personal information with tools at home like a locking mailbox, an in-home safe for storage, and a shredder for disposal of personal documents.**

☐ **We will install cybersecurity safeguards like:**

- ○ **Passcodes and screensavers**
- ○ **Firewalls**
- ○ **Antivirus and encryption software**
- ○ **Secure passwords**

☐ **We will consistently download updates for security patches and use strong passwords and change them often.**

☐ **We will turn off geotagging on photos.**

☐ **We will set up filtering and monitoring software and parent protection options to block inappropriate contacts on the Internet and filter and monitor child online activities.**

Best cybersecurity practices:

☐ **We are aware of cybersecurity risks:**

- ○ **Tracking**
- ○ **Malware (viruses, adware, spyware, Trojan horses)**
- ○ **Scamming**
- ○ **Phishing**
- ○ **Hacking**
- ○ **Identity theft**

☐ **We will frequently backup our data to avoid loss or corruption of files.**

☐ **We will not disclose identifying personal information online, like:**

- ○ **Name**
- ○ **Address**
- ○ **School**
- ○ **Date of birth**
- ○ **Or any other personally identifying information in images (t-shirts with our school logo).**

☐ **We will not click on embedded links or open, copy, or share attachments from unknown sources.**

If we are outside of the house, we agree that:

- □ **We won't post pictures that reveal travel data, like boarding passes, passports, or travel or hotel vouchers.**
- □ **We will wait until we're home to post travel photos.**
- □ **We will practice *situational awareness*, because we understand people can read screens over our shoulders.**
- □ **We will avoid public WiFi unless staff at the public place tells us the WiFi source is legit. This is because cybercriminals can sidejack our online transmissions with criminal tools and software.**
- □ **We will avoid online tasks that involve private information like online banking or using private transaction information like date of birth, credit card numbers, or social security numbers when we are in a public place.**
- □ **We will always log out when using a hotspot to avoid a hacker tapping in and continuing the session.**
- □ **We will avoid using public computers for the same reasons it's risky to use public WiFi. Software could be silently running in the background, thus capturing data from our online activities.**
- □ **We will turn off location data on social media apps (like going "ghost mode" on Snapchat).**

______________________________ ______________________________

Kid Signature ***Parent Signature***

______________________________ ______________________________

Date ***Date***

Here are some helpful materials to help you get prepped for your cybersecurity family talk:

Definitions for concepts that are included in the cybersecurity section of your GKIS Connected Family Agreement

Malware is any software that attacks or captures data on your computer. These include viruses, worms, Trojan horses (links that look like beneficial downloads, but are actually malicious), spyware, adware, and other malicious programs.

Hacking is unauthorized computer or smartphone access to get data or images or even hijack the camera or mic for secret recording.

Phishing is a type of scamming that is a fraudulent attempt, usually through telephone, email, instant messaging, or a website, to gain sensitive personal information like login credentials or credit card information. Stolen information is then used for fraudulent activities like stealing money, credit card fraud, stealing your identity, or launching further phishing scams. Phishing attempts are often difficult to identify, because the fake website or email can look nearly identical to a legitimate one, such as posing as a popular website, auction site, online payment processor, or IT administrator.

Scamming is a con to get something from an unsuspecting victim. A common scam is posing as the IRS to convince the victim to wire money or be prosecuted for unpaid fees or taxes or suffer frozen bank accounts.

Great GKIS Articles About Cybersecurity (for parents)

Child Identity Theft is on the Rise. Protect Your Family Against Cybercrime

Virtual Kidnapping, A Parent's Worst Nightmare. How to Protect Yourself and Your Family.

Can Your Phone Get a Virus From Texting? GKIS Parent Beginners Guide to Texting and Instant Messaging (IM)