TRUSTED FUTURE

LEAD BY EXAMPLE — ADOPT BASIC CYBER HYGIENE BEST PRACTICES

Parents often inherently understand that one of the most effective tools for raising savvy and responsible adults is to lead by example. Our children learn by watching what we do, how we do it, and why – especially when it comes to technology. While parents are already doing a lot to engage their kids, Trusted Future research also found that parents can do much more in terms of leading by example and modeling positive practices. Only about half of adults are following basic cyber hygiene best practices – practices like adopting strong passwords, using multifactor authentication, only downloading from official app stores, and avoiding clicking on untrusted links. In the same way we teach kids to look both ways before they cross the street, now we need to teach them to think twice before they click an un-trusted link.

Making safe and healthy technology use a family project, not just something you expect of your kids, can help improve safety, security, and privacy for the whole family.

1 **ADOPT STRONG AND UNIQUE PASSWORDS FOR ALL ACCOUNTS, INCLUDING "SHARED" FAMILY ACCOUNTS.**

As a rule, passwords should be unique and strong for every account—including video and other entertainment apps used collectively by the family. Password manager programs can help you create—and remember—complex passwords for each account. These programs will also alert you if your accounts are compromised or passwords are found in a data leak.

2 **MODEL SAFE BROWSING BEHAVIOR.**

Both kids and parents should avoid visiting insecure websites, clicking on untrusted links, or downloading unvetted software and apps. Browsers will show a "lock" image by the website's URL to help you quickly confirm that a website is using HTTPS.

3 **ONLY DOWNLOAD APPS FROM TRUSTED SOURCES.**

Mobile malware is on the rise and is primarily delivered via malicious apps available outside of official app stores. In contrast to the apps in Android's Google Play and Apple's App Store, which are reviewed by experts for safety and security, apps that are downloaded from outside

of official app stores have not been reviewed by experts and are not bound by the consumer protection requirements built into app store guidelines. Configuring a device to "sideload" apps from outside official app stores, a practice that is possible but discouraged for Android users, can also make a device more vulnerable to malware if a user mistakenly clicks on an untrusted link.

4 MAKE SURE YOU UNDERSTAND HOW YOUR DATA (AND YOUR FAMILY'S DATA) WILL BE USED BEFORE DOWNLOADING AN APP OR GIVING AN APP PERMISSION TO ACCESS CERTAIN DATA.

Only 16% of respondents in a recent Trusted Future survey felt very in control of their privacy. To gain better control, before you or your child downloads an app, review the privacy label for the app in the app store to be able to quickly see and compare what data it collects and for what purposes. If it collects extraneous information unrelated to the purpose of the app, or if it is too vague about what data it collects, you can choose to use a different app.

- *When apps ask for permission to access certain data, take the opportunity to talk with your kids about why it is important to think carefully before granting an app access to certain data and to reject requests asking for extraneous information.*

5 TEACH YOUR KIDS HOW TO DISTINGUISH TRUSTWORTHY AND UNTRUSTWORTHY ONLINE SOURCES OF INFORMATION.

A Stanford study found that 82% of middle school students can't differentiate between ads and actual news on a website. Providing children with the basic skills they need to make more informed decisions about what online content to trust not only enables better digital literacy, but can also help children avoid online scams, perform better in school, and steer clear of harmful online misinformation. As kids progress in school, they will also learn about the importance of using reliable sources when writing research papers and working on other school projects. Set them up for success in college and life by teaching them how to spot fake news, how to tell whether a site is a trustworthy source, and reinforcing these concepts early and often. These are especially helpful skills if they are using social media or frequent video streaming platforms, both places where misinformation, disinformation, and/or malinformation is ripe.

Misinformation is false, but not created or shared with the intention of causing harm.

Disinformation is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.

Malinformation is based on fact, but used out of context to mislead, harm, or manipulate.

Source: Cybersecurity and Infrastructure Security Agency

- ***Do it together:*** *Take advantage of opportunities in everyday life to model being a sophisticated consumer of online news and information. For young kids, narrate out loud why you are using certain websites over other sources.*

ADDITIONAL RESOURCES:

TRUSTED FUTURE

8 Steps to Better Protect Your Privacy Online

9 Essential Steps to Keep Your Device Secure

5 Key Steps: How to Stop your Mobile Activity from Being Tracked

WATCH: Trust Talk: Protecting Child Safety

AMERICAN PSYCHOLOGICAL ASSOCIATION

Digital guidelines: Promoting healthy technology use for children

COMMON SENSE MEDIA

Parents' Ultimate Guide to Parental Controls

Privacy and Internet Safety

How do I decide which parental controls to use?

Should I let my tween girl use social media?

What are the basic safety rules for cellphones?

CONNECTSAFELY

Family Guide to Parental Controls

FAMILY ONLINE SAFETY INSTITUTE

How to be a Good Digital Parent Toolkit

IKEEPSAFE

Guidance for the Safe and Healthy Use of Technology – Youth/Parent Fireside Chat

CISA

Keeping Children Safe Online

Staying Safe on Social Networking Sites

Parents and Educators Tip Card

Chatting with Kids about Being Online

FBI

Keeping Children Safe Online

FTC

Kids and Mobile Phones

Talk to Your Kids

Kids and Computer Security

Parental Controls

Protecting Your Child's Privacy Online

Kids: Texting and Sexting

Kids and Socializing Online

USA.GOV

Online Safety in the Age of Digital Learning

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

12 quick online privacy tips for parents

CANADIAN CENTRE FOR CYBER SECURITY

Cyber security for kids: How parents can talk with their children

AUSTRALIA'S ESAFETY COMMISSIONER

Parents, Young People, & Kids

NATIONAL CYBERSECURITY ALLIANCE

Tips for Parents on Raising Privacy-savvy Kids

INTERNET MATTERS

Helping parents keep their children safe online

KQED

How Parents can Model Better Screen Time Behavior for their Kids

NY TIMES

How and When to Limit Kids' Tech Use

PBS

Online Safety Tips for Parents

CONSUMER REPORTS

Internet Safety for kids: How to Protect your Child from Online Danger

How to Use the Parental Controls on a Smartphone

trustedfuture.org