TRUSTED FUTURE

EMPOWER YOUR KIDS TO BECOME SECURITY-SAVVY

During the pandemic we saw just how important digital devices can be for kids as their tablet became a gateway to their classroom, enabling them to swipe their hand across the screen to access the whole universe of knowledge the Internet contains. But in a recent Trusted Future survey, nearly 6 in 10 adults said they lacked trust in the security of the technology that they use. Worse yet, only about half of respondents are adopting the basic cyber security practices recommended by experts. Given that human error is the main cause of 95% of cybersecurity breaches, we all stand to gain from adopting these basic best practices.

Like adults, kids can become victims of cybercrime, have their accounts compromised, their digital privacy violated, or their identities stolen. Despite their tech savvy, children can be especially vulnerable to social engineering attacks and other forms of online manipulation. With mobile malware on the rise and smartphones in the hands of almost every teen, more and more kids are getting messages trying to trick them into clicking a malicious link or downloading a free game loaded with malware.

Fortunately, Trusted Future's survey of American parents founds that large majorities recognize the importance of talking to their kids about online safety.

HERE ARE SOME PRACTICAL WAYS YOU CAN HELP YOUR KIDS STAY SAFE AND GRADUALLY BECOME SECURITY-SAVVY TECHNOLOGY USERS AS ADULTS:

1 MAKE SURE THEIR DEVICES AND ACCOUNTS ARE SECURE.

Your child's phone or tablet likely contains pictures, messages, and other sensitive content that you want to keep private. Just like you would for yourself, make sure their devices and accounts are protected by strong and unique passwords. As a family, consider using a password manager to create and remember passwords.

Kids have been known to misplace things. Don't assume that the information on your child's device isn't sensitive or couldn't be used to compromise your or their identity. Mitigate the risk by configuring their devices to require authentication before someone can access the device, such as a passcode or biometric ID. If a device is lost or stolen, immediately take advantage of any features that allow you to remotely "wipe" the data on the device.

2 TEACH YOUR KIDS TO IDENTIFY SIGNS THAT A TEXT MESSAGE, WEBSITE, APP, OR ONLINE STORE IS INSECURE OR UNSAFE.

It is critically important that parents drive home the importance of being cautious, especially before clicking on a link. Cybercriminals are increasingly targeting children and teenagers with social engineering attacks, raising the importance of teaching kids to be cautious when using tech or surfing the web. Show them how they can identify secure websites that use HTTPS by either checking the beginning of the website's URL or looking for the image of a lock. When you get phishing messages, point out suspicious attachments, poor grammar, spoofed links, and any other red flags so your kids learn what to be on the lookout for. Talk to them about how criminals will try to trick them by posing as a trustworthy or "official" source, like their school. Show your child how to block phone numbers and how they can report spam or scam texts on the FTC's website.

IN OUR RECENT SURVEY,

of parents believe that it is important to tell young kids to think twice before they click on a link, just like they tell their kids to look twice before crossing the street.

3 MAKE CLEAR THAT KIDS SHOULD NEVER SHARE SENSITIVE PERSONAL INFORMATION ON SOCIAL MEDIA.

Even if the audience for a post is limited, both parents and kids should avoid sharing personally identifiable information on social media. Cybercriminals or other bad actors can use the information to piece together details about your family, which can make it possible for them to answer security questions necessary to access financial and other accounts. It is also good practice to avoid tagging a precise location when posting photos of your child. Encourage your kids to do the same.

4 EMPOWER YOUR KIDS.

You can empower your kids to protect themselves by teaching (and modeling) good cyber hygiene practice. Teach them how to identify and avoid inappropriate content, websites or links that appear unsafe, or apps and games that come from an untrusted source. And because content filters are imperfect, talk to your kids as they begin to use the internet more independently about sexual and other inappropriate content and what they should do if they encounter it online.

Just like you teach your child to call 911 in an emergency, train your kids about how they should respond to unwanted or harmful content. Show them how to block numbers responsible for harassing, unsolicited, or unwanted calls or texts. Make sure they know how to use the various reporting tools on the social media sites and other platforms that they frequent.

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