Keeping Kids Safe on Social Media + 10 Tips for Parents

Text Message Scams

The rise of unsolicited text messages is bringing on another form of scamming that puts your personally identifiable information (PII) at risk. Usually, it's a bogus message, such as your bank claiming your account is locked and you need to call a certain number and give certain credentials. Or it's a link to claim a prize you've supposedly won—clicking the link installs malware on your phone that gives criminal hackers access to your PII. To avoid being scammed, simply think before you click, and check out the **Federal Trade Commission's** list of how to protect your personal information.

EMAIL SPOOFERS ARE GETTING SMARTER

Even the most security aware folks can get spoofed when scammers are good at what they do. ***"The email was surprisingly well written without the spelling and grammar errors I have come to expect from fake emails."*** That says it all; scammers are getting better at getting clicks. Which means we need to get better at vetting. Think before you click, and when in doubt delete! Read the whole story by visting the link below.

thesecurityawarenesscompany.com/2016/02/03/scam-alert-help-i-had-an-easter-disaster-in-the-philippines/

Smart, secure networking starts at home and it starts early. At some point, our children will reach the age where they're old enough to develop an online presence. It's up to us as parents to educate them about the dangers associated with these networks, and how important it is to protect that online presence.

In order to do that, we need to educate ourselves on every social media network our children are joining. That means joining the network and boning up on how information is shared, so that we can teach them how to protect their accounts in addition to teaching them why what they share matters.

We don't necessarily want to scare our children, but making them aware of the dangers ahead is part of our jobs as parents. For that reason, showing them examples of how their shared information can be used against them, and introducing them to concepts like cyber bullying and stalking, can be a fantastic way to educate them. If they are aware of the consequences, they will make smarter choices.

No idea where to begin? Try these conversation starters:

thesecurityawarenesscompany.com/2015/11/18/conversation-starters-for-kids-receiving-tech-gifts/

1. **Don't assume your child knows more than you about navigating technology.**
2. Make sure your kids know what is and is not appropriate to post.
3. **Don't post personal financial information such as credit and debit card numbers, bank statements and pay checks on social media.**
4. Don't post other personal, non-financial information on social media, such as a new driver's license.
5. **Don't post information about the place you work.**
6. Don't post your social plans and vacation details.
7. **Don't let your kids "check-in" everywhere they go.**
8. Know with whom your kids are connecting.
9. **Monitor your kids' credit reports.**
10. Be actively involved in your child's online life.