BOY SCOUTS OF AMERICA®
HEALTH AND SAFETY

BSA SAFETY MOMENT
CYBER SAFETY

SUMMARY

Today all of us are spending more time than ever using digital media for education, research, socializing, and fun. Keeping safe online has become more important than ever. To help families and volunteers keep youth safe while online, the Boy Scouts of America introduced the Cyber Chip. In developing this tool, the BSA teamed up with content expert NetSmartz®, part of the National Center for Missing and Exploited Children® and training expert for many law enforcement agencies.

GENERAL INFORMATION

The Cyber Chip can be used as a tool to show skill and a commitment to do what's right in the cyberworld. Many unit leaders use the Cyber Chip before allowing any electronic use on outings—this is a decision each unit can make on its own.

The Department of Homeland Security has provided a number of practical tips to protect Scouts and Scouters from cyberattacks:

Never click on links in emails. If you do think the email is legitimate, whether from a third-party retailer or primary retailer, go to the site and log on directly. Whatever notification or service offering was referenced in the email will be available via regular logon if it was valid.

Never open the attachments. Typically, retailers will not send emails with attachments. If there is any doubt, contact the retailer directly and ask whether the email with the attachment was sent from them.

Do not give out personal information over the phone or in an email unless completely sure who you are giving it to. Social engineering is a process of deceiving individuals into providing personal information to seemingly trusted agents who turn out to be malicious actors. If contacted over the phone by someone claiming to be a retailer or collection agency, do not give out your personal information. Ask them to provide you their name and a callback number. Just because they may have some of your information does not mean they are legitimate!

Verify the authenticity of requests from companies or individuals by contacting them directly. If you are asked to provide personal information via email, you can independently contact the company directly to verify this request.

Set secure passwords and don't share them with anyone. Avoid using common words, phrases, or personal information and update them regularly.

Keep your operating system, browser, anti-virus software, and other critical software up to date. Security updates and patches are available free of charge from major companies.

Pay close attention to website URLs. Pay attention to the URLs of websites you visit. Malicious websites sometimes use a variation in common spelling or a different domain (for example, .com instead of .net) to deceive unsuspecting computer users.

Turn off the option to automatically download email attachments.

Be suspicious of unknown links or requests sent through email or text message. Do not click on unknown links or answer strange questions sent to your mobile device, regardless of who the sender appears to be.

REFERENCES

- Department of Homeland Security, "Stop.Think.Connect Videos": www.dhs.gov/gallery/stopthinkconnect-videos (videos about safety online)
- Department of Homeland Security, "Protect Myself from Cyber Attacks": www.dhs.gov/how-do-i/protect-myself-cyber-attacks
- BSA, "Cyber Chip": www.scouting.org/training/youth-protection/cyber-chip/