GRANDPARENT'S GUIDE TO TECHNOLOGY

VOLUME 3

SAVVY CYBER KIDS

SAVVYCYBERKIDS.ORG

FROM A TO Z:
TECH TERMS EVERY GRANDPARENT SHOULD KNOW

While technology often brings us together, it can also drive us, generationally, apart. The challenge of getting tech advice from your children and grandchildren can sometimes result in family moments best forgotten, and quickly. Yet, you can be "cool" in the eyes of your grandchildren by using technology to spend quality one-on-one time cultivating a close relationship. The grandparent "special sauce" is figuring out how to consistently and continually entertain, educate, support and make yourself relevant to your grandchildren's lives in unique and interesting ways. Fear not, Savvy Cyber Kids is here to help with a glossary of tech terms and concepts that will improve your 'connectivity' with the tech generations.

AI or ARTIFICIAL INTELLIGENCE is defined as "the theory and development of computer systems able to perform tasks that normally require human intelligence." AI computers are designed to be intelligent machines who work and react just like humans; they can learn, plan and problem-solve. What does AI mean in your life today? Think about mobile check deposits through a smartphone app that rely on technology to decipher and convert handwriting on checks into text; traffic predictions in Google Maps or Waze to reduce commute times; and commercial airlines that rely on AI to pilot plans. In fact, as The New York Times reported, the average flight of a Boeing plane involves only seven minutes of human-steered flight, which is typically reserved only for takeoff and landing. Facebook uses AI for facial recognition in suggesting who to tag in an uploaded photo. Voice-to-text features on smart phones rely on AI-powered voice recognition.

BLOCKCHAIN is a decentralized digital ledger of all transactions across a peer to peer network. Using this technology, participants can confirm transactions without a need for a central clearing authority (no bank!). While potential applications can include fund transfers, settling trades, voting, and many other issues, Blockchain is best known as the technology that enables the existence of cryptocurrency.

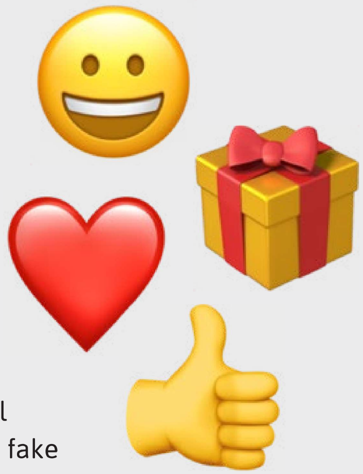
CRYPTOCURRENCY is a medium of exchange, such as the US dollar, but is digital and uses encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin is the name of the best-known cryptocurrency, the one for which blockchain technology was invented.

CYBER SAFETY means engaging in behaviors online that keep you safe, maximizing your personal safety and minimizing security risks to your private information, including self-protection from computer crime. When you think about your grandchildren, true digital natives who are accustomed to a world connected to technology and technology's influence on our daily activities, cyber safety means growing up cyber aware embracing respect and empathy as it relates to digital decision-making. Savvy Cyber Kids provides free resources for grandparents, parents and teachers to educate children on numerous cyber safety concepts such as personal safety, self-image, bully response, technology balance, appropriate use, digital reputation and privacy.

DM refers to private conversations on social media platforms. Instead of posting a message to someone's feed, say on Twitter, Facebook or Instagram, you can DM or direct message someone so that only they can view the contents of the message.

ENCRYPTION converts information or data into a code and is most typically done to prevent unauthorized access, in other words, to protect sensitive information that is transmitted online by not allowing the information to be accessed by unauthorized users. It is widely used on the internet to protect user information being sent between a browser and a server, including passwords, payment information and other personal information that should be considered private.

EMOJIS are standard fare in electronic communications these days and refer to a small digital image or icon used to express an idea or emotion in an email or text. The meaning of emoji's can be contextual, so be careful what you post. Since new emoji's are released regularly, it can be hard to keep up.



FAKE NEWS refers to false information or propaganda published in a manner so that it is seen as authentic news. This is a technology term as social media and fake news websites are associated with fake news. They push their fake news content to mislead consumers and spread misinformation via social networks and word-of-mouth. PolitiFact says: "Fake news is made-up stuff, masterfully manipulated to look like credible journalistic reports that are easily spread online to large audiences willing to believe the fictions and spread the word." Politics aside, when you are speaking to your grandchildren about fake news, you can discuss the critical thinking skills needed to sort through the vast amount of information that come from their digital worlds. Ask them how their teachers address this topic and recommend they research news sources to determine fact from fiction.

GAMING refers to electronic games or video games on game consoles like Xbox and Playstation or on personal computers (then it's known as online gaming). Pong, an electronic version of ping pong, was introduced in the 1970's and was the first widely played video game. Since then, gaming has grown increasingly complex with enhanced graphics, full-motion video, 3-D effects, high fidelity stereo sound and much, much more (think immersive play, virtual reality and motion gaming that responds to the movement of users). Thanks to high-speed internet, multiplayer games are now designed to meet the playing demands of up to hundreds of thousands of online users simultaneously. Is your grandchild a gamer? Odds are that he or she is. Gaming is a major industry. Worldwide video game sales approached 75 billion in 2015 and are expected to reach 90 billion by 2020. In 2014, there were 1.8 billion gamers in the world—that's 25 percent of the entire global population! The negative sides of gaming get a lot of press. Gaming faces criticism by groups who point out that some of the programs have violent, xenophobic, sexually explicit or otherwise objectionable content. Concern has also arisen because some young people seem to become addicted to gaming, spending inordinate amounts of time at the activity. That said, gaming isn't all bad. It can be useful in a wide variety of professional and educational scenarios, especially in simulations for activities requiring visual and motor coordination such as driving race cars and piloting military fighter aircraft. Gaming can also help kids with their long-distance relationships with friends and families. As a grandparent, gaming affords you an opportunity to get involved in your grandchild's digital life. Ask your grandchildren about what kinds of games they play and why!

HEALTHCARE SCAM is when your Medicare ID or health insurance member number is used to get medical services, or to issue fraudulent billing to your health insurance provider. If you believe you have been a victim of medical identity theft, call the Federal Trade Commission at 1-877-438-4338 (TTY: 1-866-653-4261) and your health insurance company's fraud department. You can create a complaint form with the details of your experience at IdentityTheft.gov to share with them and with law enforcement. If you suspect that you have been the victim of Medicare fraud, contact the U.S. Department of Health and Human Services' Inspector General at 1-800-447-8477. There are steps you can take to prevent identity theft and freezing your credit is one of the most important safeguards.

HTTPS is the Betty Crocker Seal of Approval that tells you that you are visiting a safe website. If there is a green lock icon next to the URL address, then you are on a page protected by HTTPS, or Hypertext Transfer Protocol Secure. What does that mean? Sites that use HTTPS have a Secure Sockets Layer (SSL) which prevents your sensitive information from being stolen or spied on. This is especially important if you are visiting a website while on a public Wi-Fi. If that is the case, don't enter any sensitive data on non-HTTPS sites while on a public Wi-Fi.

INTERNET OF THINGS (IoT) refers to the interconnection via the Internet of computing devices embedded into everyday objects, like vehicles, home appliances and toys, enabling these devices to send and receive data. IoT can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, cameras streaming live feeds of wild animals in coastal waters, automobiles with built-in sensors, DNA analysis devices for environmental/food/pathogen monitoring, or field operation devices that assist firefighters in search and rescue operations. IoT is often hailed as a source for a next-level set of innovations that will directly benefit seniors. These are “smart” devices that connect in the digital landscape and help monitor, alert, track and support seniors. The idea behind the innovation is that these devices will keep seniors connected and safe—and help alleviate some the stress on the professionals and caregivers supporting them.

IRL stands for **In Real Life**. From a cyber safety perspective for kids, this term is applied to friends, distinguishing between friends on gaming and social media platforms, who may, in fact, be strangers with whom no personal information should ever be shared and people kids know in real life, family members, schoolmates and sport team friends.

JACKPOT LOTTERY SCAMS are when you receive an email from an official-looking lottery. The subject line offers a congratulatory announcement and alerts you to money you've “won.” You can bet your winnings are false if the sender is a person, your name is not in the “to” field, the lottery doesn't exist online and if the email requests your personal information. This is a great example of, if it sounds too good to be true, it usually is! If someone you don't know is reaching out to you electronically with offers of cash and reward, be concerned that it is a scam. Above all, don't respond to unsolicited requests for personal information (your name, birthdate, social security number, or bank account number) by phone, mail, or online. Remember, just because someone is asking does not mean you need to answer. In fact, if someone you don't know is asking for personal information, that is a red flag. Use a critical eye and stop to ask yourself what is really going on.

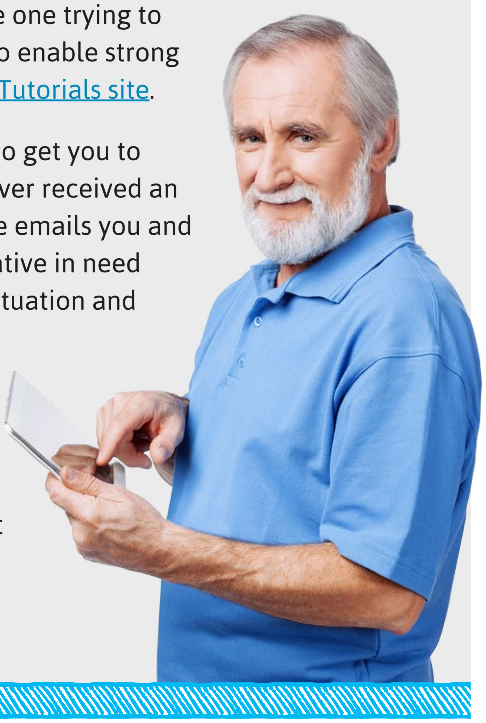
KNOWLEDGE ENGINEERING is a central aspect of AI research. Machines can be designed to act and react like humans only if they have access to a mass of information relating to the world. So, an artificial intelligence machine must have information about objects, categories, properties and the relations between all of them, in order to implement knowledge engineering, and, in other words, be intelligent. This imitation of human reasoning, giving machines the ability to initiate common sense, reasoning and problem-solving powers, is the greatest challenge for taking AI from concept to everyday life.

LINK – To protect everything that you have that is worth stealing, fight your basic instinct to click and open anything sent to you. Take a moment to think about the action you are about to take. Should you really click that link? The reality is that not all links should be clicked because they could be ransomware or a virus. Verify the person or organization that sends you an email, text, or social media message with a link or attachment to click ACTUALLY sent it (and it was not forged by someone with malicious intent). You can call them or go directly to the website being used. As an example, if you receive an email from your bank or email provider asking you to reset or verify your password, open a new browser page and type the main service provider site address yourself and then login to see if indeed they need you to take any action. Be aware and stay vigilant.

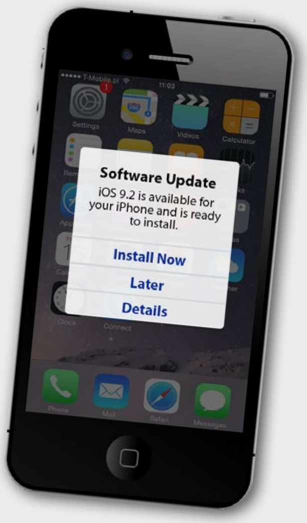
MACHINE LEARNING is another core part of AI research; the premise that machines can learn without any kind of human supervision. Machine learning means that computers can be designed to identify patterns in streams of inputs, and make decisions based on these patterns. Machine learning is the specific scientific method currently in vogue for building AI. What does machine learning mean in your life? Think about ridesharing apps like Uber and Lyft that use machine learning to determine the price of your ride, minimize wait time when you ask for a ride, and optimally match you with other passengers when you select pool. Spam filtering also relies on machine learning to go beyond simple rules-based filters, filtering out messages with words like “Nigerian prince” or “online pharmacy” that spammers can easily avoid by removing those words, to instead have machine learning based filters that continuously learn from a variety of signals, such as the words in the message, message metadata (where it’s sent from, who sent it, etc.) and your own specifications. It is only through the use of machine learning algorithms, that Gmail can successfully filter 99.9% of spam.

MULTI-FACTOR AUTHENTICATION is a way of strengthening your passwords and access to websites that contain your personal information (also called strong authentication or 2 factor authentication) and should be enabled on ALL accounts that accept it. The multifactor aspect can come in the form of a text message sent to your phone, an email sent to the address you have on file with a service provider, a challenge request from an authenticator app, such as DUO, a voice call to a phone number on record, or another way to verify that you are actually the one trying to gain access to your account and not an imposter. For instructions on how to enable strong authentication across multiple services, review the information at the 2FA Tutorials site.

NO GOOD DEED GOES UNPUNISHED refers to help scams that try to get you to panic and act quickly without calmly considering the situation. Have you ever received an email sent by a relative or friend asking for help? It goes like this...someone emails you and provides some basic information that convinces you that they are your relative in need of help, know your grandchild or loved one and that he or she is in a dire situation and needs immediate financial help because of an accident or emergency. Or maybe someone you have connected with on an online dating website reaches out to you and needs your help with travel expenses so that you can meet for the first time in “real life.” The scam artist will ask to have money wired directly into his or her hands. In reality, your grandchild is perfectly fine and your love connection isn’t who you thought he or she was. Be wary, be very, very wary of online pleas for help!



OPERATING SYSTEMS are an important part of how hackers get to you. Updating your software the first chance you can is crucial to protecting yourself from cyberattacks—and it's easy! I bet you get them all the time—those annoying popups that invite you to install the latest update on your phone, tablet or computer. The notifications typically come at inopportune moments and because the popup is an interruption, the natural response is to hit "Remind Me Later" instead of installing the update upon first notification. Second guess that decision! Each time you receive a notification that an update is available for the software that runs on your device, you should proceed with the update promptly. The updates—and they come from manufacturers such as Apple, Microsoft, Alphabet (formerly known as Google), Adobe and many others—typically mean that a security flaw has been discovered in the specific product you are using and that a fix to the security flaw has been created. The only way to get the fix on your device is to install the update.


Software Update

iOS 9.2 is available for your iPhone and is ready to install.

PASSWORDS, when done correctly, can help ensure you and your family members are not an easy target for the online scams. Stop reusing passwords. I know this a challenging request based on the many logins necessary every day, each one typically requiring you to authenticate yourself and prove it is you trying to log in by using a username and password.

PASSWORD MANAGER – To save you from having to remember hundreds of username and password combinations, use a reputable password manager such as Password Safe. With a password manager, you only have to remember one password with the benefit of having vastly improved security AND convenience.

PHISHING is a common hacking technique and involves an adversary crafting an email, text message, or social media message that is written in such a way that you are compelled to click the link or open a document that is part of the message. The next step typically involves you entering your authentication details to access a bank account, email account, social media account, or any other online service. The temptation to click and open anything has made phishing the most widely used technique to get people to give up their access credentials. Verify that the person or organization that sends you an email, text or social media message with a link or attachment to click is the real sender. You can call them or go directly to their website—don't click the link and assume that the website it takes you to is authentic. For example, if you receive an email from your bank or email provider asking you to reset or verify your password, open a new browser page and type the main service provider site address yourself and then login to see if indeed they need you to take any action. One general caveat: Most reputable businesses and organizations don't send you emails requesting you to reset your password unless you've already told them that you've forgotten it. So if you receive such an email, chances are good that it's a fake. Other tips on how to spot a phishing email:

- Bad grammar is a tell-tale sign that something is off.
- If the sender's email is a little unusual, like bancofamerica.com or bankkofamerica.com instead of bankofamerica.com, it's not an email from Bank of America.
- If the link you are be invited to click on looks different than what you expect it to be, be wary. Hover your mouse over the link and you will see the web address that you would be sent to if you clicked on it. If the web address is going to a suspicious website—don't click!

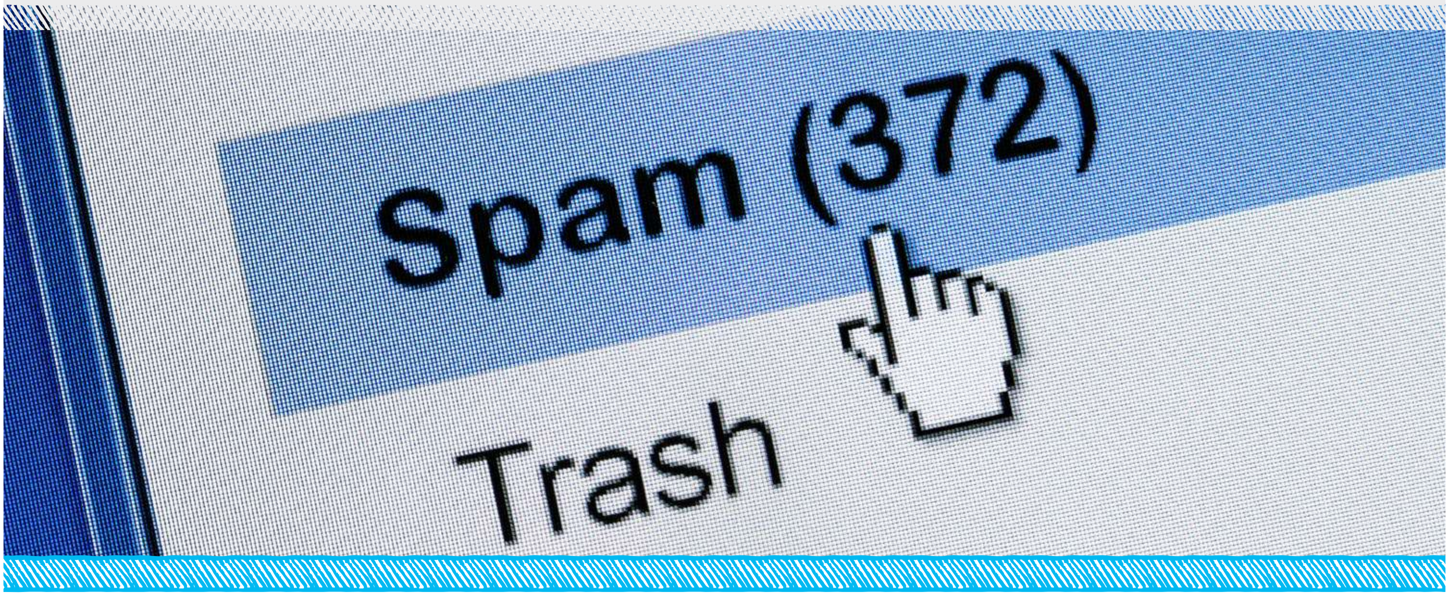
PRIVACY is a basic principle of cyber safety. If someone you didn't know approached you on the street and asked you where you lived, would you tell them? Probably not. If they asked you where you banked and for your account number and online banking password, would you consider giving out that information? Very unlikely. Face-to-face and in real time, we tend to be good at protecting what is important to us. Somehow, these same questions and intrusions on the screen of our devices can seem less invasive and safe enough to embolden us to share our most valuable assets—our personal data. Keep your private information, private!

QUESTIONS – Ever wonder if what you are reading is fake news? If you have questions, visit www.snopes.com. Begun as an urban legends reference site, www.snopes.com now can help you sort through newsworthy information to test it for rumor or truth.

RANSOMWARE is one of the more vicious tools in a hacker's arsenal. It takes over your computer and threatens you with harm, most typically denying you access to your data. The hackers deploy ransomware via a phishing scam where you click on a link thinking it is safe and then unknowingly give the criminal access to your computer or the hackers gain access by exploiting a security hole in your operating system. Once in control, the hackers will demand a ransom before they will relinquish access to you.

SNAP refers to Snapchat or an image on Snapchat, a universally popular social media platform that your grandchild is more than likely active on. One popular feature of snapchat are its facial features which track facial movements, and allow users to add animated effects or digital masks that adjust when their faces moved. This technology is powered by machine learning. If you have heard the term "streaks," this refers to sending a snap to your friends everyday without missing a day. The longer the streak, the better (in your grandchild's mind).

SPAM ACCOUNT can mean different things depending on your age. You may already be familiar with a spam account as a secondary email account that is used for sign-up pages when people don't want to give their primary email address, and use this account to avoid promotional emails that have little or no value. For your grandkids, a social media spam account can be a way for them to post whatever they'd like online without parental interference. It's a secret account that they only allow to be followed by the friends they want to know about it.



TARGET – Don't be the next victim of an online scam by putting out too much personal information on social media, like when you are going on vacation, who you are going on vacation with and how empty your house will be. Be safe out there! Many scammers specifically target seniors, assuming that you are unfamiliar with the ways of the web and are easier to con. If you've fallen for an online scam, you are not alone. Looking ahead, you can protect your identity and your money by arming yourself with knowledge and avoid falling prey to scammers.

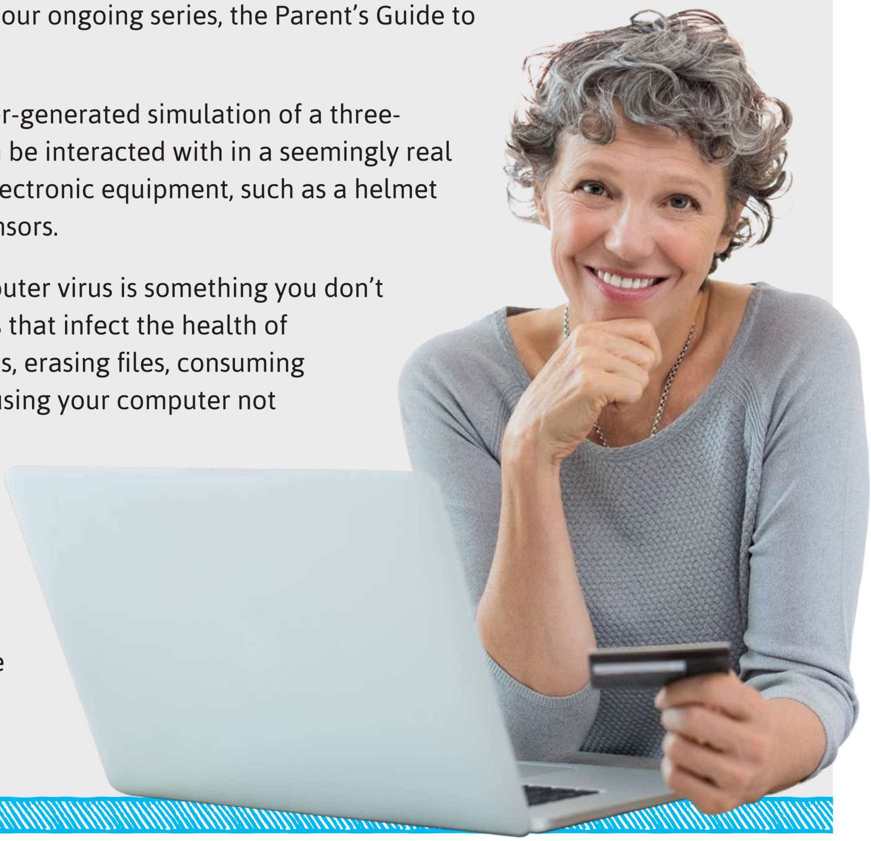
Consider this your 30-second "tech talk" for safety basics (and I bet it sounds familiar to advice you have given family members!).

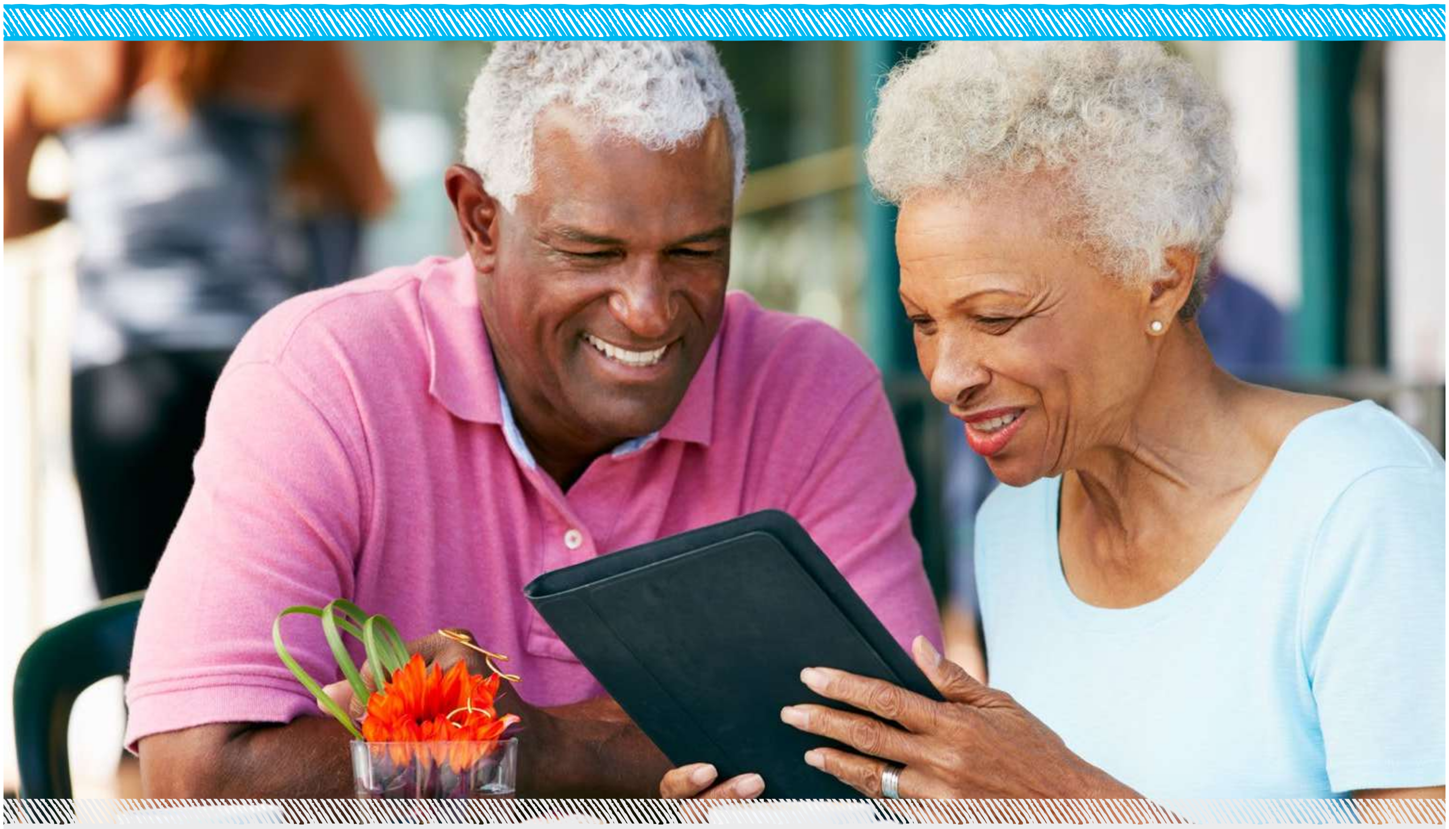
- Don't share personal information.
- Don't talk to strangers.
- Beware of things that sound too good to be true.

(U)YOU... From time to time, Savvy Cyber Kids will discuss software and hardware parental controls that are aids to digital parenting. They can never replace the best parental control...YOU are the best (grand) parental control there is. When your grandchildren visit, talk to them about technology, ask questions and be inquisitive about what they are doing in their online worlds. They need you. There is no one-stop shop set of rules for digitally parenting. Every family can and should make their own judgements, even from child to child, about what constitutes cyber safety and cyber ethics in the family home. The one rule we impart to EVERY digital parent is to get involved and stay involved in your children's digital lives. No matter what level of technical control you put in place inside and outside your home, the influence of tech and mass media is breezing past you outside the home—maybe even on your child's devices. Your child is being exposed to images and messages that you should be aware of. Children need a parent (and a grandparent) by their side helping them to navigate this new world. To get started, visit our website SavvyCyberKids.org and sign up for our ongoing series, the Parent's Guide to Technology, under Free Resources.

VIRTUAL REALITY or VR is the computer-generated simulation of a three-dimensional image or environment that can be interacted with in a seemingly real or physical way by a person using special electronic equipment, such as a helmet with a screen inside or gloves fitted with sensors.

VIRUS – Just like a biological virus, a computer virus is something you don't want to get. Computer viruses are programs that infect the health of your computer, by creating files, moving files, erasing files, consuming your computer's memory, and generally causing your computer not to function correctly. Some of the more insidious viruses can duplicate themselves, attach themselves to programs, and travel across networks. Opening an infected e-mail attachment is the most common way to get a virus. Want to stay healthy? Install and regularly update a antivirus program on your computer.





WiFi – Let's talk about public WiFi hotspots. The best advice is to use them sparingly! Stick with using your cell phone when out in public areas to avoid having your actions monitored by others in the area or trick you into logging into a site that will steal your information. If you must use public WiFi hotspots, use a VPN service as soon as you connect. But the best solution for using your non-cellular connected device on the go is to turn on the hotspot functionality on your cell phone. Then, connect that non-cellular connected device, usually a laptop of tablet, to the wi-fi connection on your phone. This way, you will be the only one connected to your private wifi network.

WRONG – You need to remind your grandkids that they can easily make a wrong decision on the internet and it can have a lasting, negative impact on their lives. From making inappropriate jokes to sharing or commenting on images that are offensive, your grandchild's wrong decision can get them kicked off a sports team, unaccepted from a college and even national notoriety.

WISDOM – As a grandparent, you can impart wisdom on your grandkids and encourage them to use their cyber super powers for good. When it comes to digital grand-parenting, remember that today's kids don't know how to make smart decisions unless someone discusses cyber ethics topics with them. The reality is that your grandchildren's social world is now predominately online, where few adults can track it, and their cyber relationships are highly susceptible to negative interactions. It's ok for you to set technology boundaries with grandchildren in your home. But remember, the ways your grandchildren interact with technology outside of your home are even more important for their safety. Even if your grandchildren are older and have been immersed into screens, virtual worlds and all that technology has to offer for years, it's not too late to have the "Tech Talk." Your grandchildren are entering adulthood in a world defined by technology. As a grandparent, it's imperative that you provide your grandchildren with the tools to be cyber aware.

(X)CROSS ROADS – Your grandchildren live at the crossroads of technology, with equal access to all good and bad that technology has to offer. You need to show them how to use technology for good and how to avoid the mistakes that are bad. Kids want to interact with technology and social media is a key way tweens and teens socialize and spend their time. As a grandparent, you offer an additional source for education and are an important role model. So consider time spent with your grandchildren and technology as teachable moments. Teach your grandchildren not only how to engage safely in the digital world but also how to unplug and appreciate the world around them.

YOUNG AT HEART – No matter what new technology is developed and adored by your grandchildren, there's nothing as important as family and grandparents are an essential force in their grandchildren's lives. Get involved in your grandchildren's digital lives and join them there on Instagram, on exercise apps comparing daily steps or using digital artwork to share your point of view—find a place in their online worlds where your interests intersect.

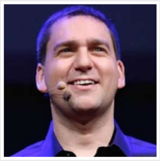
(Z) GENERATION Z – According to Forbes (2015), the generation after Millennials, Generation Z, is defined as people born from the mid-1990s to the early 2000s. They make up 25% of the U.S. population, making them a larger cohort than the Baby Boomers or Millennials and their defining characteristic is being born into a society largely defined by technology.

LOOKING FOR MORE TIPS ON DIGITALLY GRANDPARENTING?

Check out Savvy Cyber Kids' Grandparent's Guide to Technology, free via download when you sign up for our Free Resources for Parents, Grandparents and Children.

FOR MORE INFORMATION

Sign up on the Savvy Cyber Kids website for our free resources to help you navigate today's digital world with cyber ethics and cyber safety. Savvy Cyber Kids educates and empowers digital citizens, from parents and grandparents, to teachers and students.



ABOUT BEN HALPERT

By day, Ben Halpert is the VP of Risk and Corporate Security at Ionic Security, Inc. By night, he champions cyber ethics education throughout society via the 501(c)3 nonprofit Savvy Cyber Kids he founded in 2007.

ABOUT SAVVY CYBER KIDS

Savvy Cyber Kids (SCK), a 501(c)(3) nonprofit organization whose mission is to enable youth, families and school communities to be powered by technology, recognizes that children may be Digital Natives but are also Digital Naives, who, without intervention, completely lack an understanding of the implications of their digital actions. Founded in 2007 by Internet security expert, noted speaker and author Ben Halpert, Savvy Cyber Kids provides resources for parents and teachers to educate children as they grow up in a world surrounded by technology by teaching cyber ethics concepts. Savvy Cyber Kids is grateful for the ongoing support of its presenting sponsors, Digital Guardian and Ionic Security and for the support of its education series partner Earthlink.

SAVVY CYBER KIDS
4780 Ashford Dunwoody Rd
Suite A-312
Atlanta, GA 30338
SavvyCyberKids.org