CYBERSECURITY FOR OUR YOUNGER GENERATION

A review of the latest security threats and how you can avoid them

THIS MONTH'S TOPICS:

Navigating the Cybersecurity Path of Life - pg. 2

Gaming Security Tips / Learn the Lingo - pg. 3

Scam of the Month - pg. 4

It's Never Too Early - pg. 5

Cybercrime and the digital risks we face are showing no signs of slowing down. Although tools, resources, and past experiences have helped *us* prepare for some of these cybersecurity threats, the same opportunities may not be readily available to our children or the younger generation.

In order to properly prepare today's youth for the challenges ahead, try sharing your knowledge and experiences. It may seem like they have a good grasp on technology, but scams, social engineering, weak passwords and more may be subjects they know less about.

Set a strong example by flexing your cybersecurity muscles and showing off what you've learned. And, as they should feel with other life problems, make sure they know to come to you for cybersecurity questions.

NAVIGATING THE CYBERSECURITY PATH OF LIFE

Our youth will face many challenges throughout their path of life. Make sure that cybersecurity is on the agenda as an important life lesson. Before you get to the Birds and the Bees, talk about the scammers and the thieves.

START

Now is a good time for a child to learn about phishing. Teach them about phone scams, malicious text messages and emails.

Gone Fishin'
Advance 3 Spaces

This seems a bit too good to be true! Teach any children in your life this important lesson.

You Won the Lottery... even though you're 6 years old

Set up new devices with anti-virus and anti-malware protections from the get-go! Make sure these devices are kept up-to-date.

New Device for Your Birthday!

Social media should be used with extreme caution by children and young adults. Keep an eye on their friend count and look for friends they do not truly know. Parents should consider parental controls, and accounts should be set to private.

New Friend Request
Advance 2 Spaces

Viruses, malware, ransomware, and others are hard to prevent. Make sure your children know you are there for them and can help them with questions or issues.

New accounts mean new passwords. Instill strong password behaviors early in your children. Explain to them what a complex password or passphrase truly is and why they should be unique for each account.

New Account
Set Up Needed

Virus Blocked!
Advance 2 Spaces

Crypto what? Teach kids about investing, and how to do it securely. Many apps make investing easy, but scammers may be lurking trying to make an interception.

Cryptocurrency
Investment Doubled!
Advance to Finish

You Finished!!
Your child may have completed this phase of their cybersecurity journey but more scams and threats are on the horizon. Building this strong foundation of knowledge will help your child win the cybersecurity battles ahead!

Gaming Cybersecurity Tips

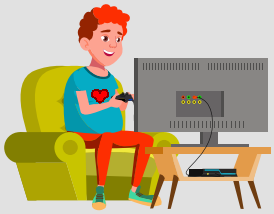
Online games are a great way for kids to have fun in a different world, but even this virtual world is filled with risks. Let's look at some popular video game categories and how their styles can relate to cybersecurity awareness.

Strategy/Puzzle - A lot of popular games focus on strategy or the player solving certain riddles. The same philosophy should be applied to cybersecurity awareness. Kids should use their problem-solving abilities to separate fact from fiction, spot suspicious links and avoid malicious traps set by scammers.

Tip: Kids are smart, but the more eyes on a puzzle, the better. Make sure they know that they can come to you with any questions they are stumped on.

Survival - Many gamers love survival games. As it sounds, the player's main objective is to survive by protecting themselves against enemies. The same logic should be applied against scammers. Kids should protect their accounts by keeping their games updated and by using strong and unique passwords.

Tip: Teach your gamer children to protect their data and accounts at all costs. Consider purchasing them a subscription to a password manager tool that can do the heavy lifting of password management for the child.



MMORPG - Although it may look like a mistyped word, MMORPG stands for Massively Multiplayer Online Role-Playing Game, the perfect genre of gaming for those that love interacting with others. With this interaction comes the risk of sharing too much personal information online. Kids and gamers using any games with a social element should treat online strangers like strangers in real life.

Tip: Avoid oversharing personal information. Scammers can play the long game to earn your trust through social engineering methods. Teach your children when to draw the line on these online channels.

Learn the Lingo, Stop the Hate

Griefers and Trolls can disrupt any player's gaming experience. **Griefers** are described as players on multiplayer online games that deliberately try to annoy other players through trash-talking, friendly fire or destruction of another gamer's reputation or created material. **Trolls**, share similar traits and mainly use verbal harassment techniques against other players. This type of behavior is not only a deterrent from a fun game, but can be very damaging psychologically to a child or young adult.

Doxxing is when a cybercriminal or nefarious rival gamer finds your personal information like your home address. Although this may be scary enough, **Swatting** can occur after this, which is when someone issues an emergency alert to local law enforcement about an active situation at your location. This is typically seen as a prank by the perpetrator but can have serious consequences. If you or your children participate in online gaming communities, this type of sensitive personal information should be kept private.

If you have a child facing online harassment, there are resources that can help. It may seem "uncool" to talk about these things with parents or a parent-like figure, but these real situations are all too common and can take a serious toll on anyone's mental health. Consider talking to the child, a therapist, mental health specialist or consult additional sources for more information.

SCAM OF THE MONTH

Each month we highlight a REAL scam that was submitted to our security team. We highlight these real examples of tactics criminals are using RIGHT NOW, that way you'll be better prepared when the next scam hits.

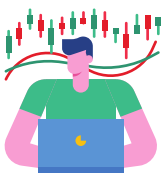
Tyler was fascinated with the huge rise in bitcoin and other cryptocurrencies. He's recently been using his phone application to invest in small portions of cryptocurrencies with some of his leftover money from his allowance and his paper route. Although he was seeing some positive returns, he wanted more. When on social media one day, Tyler saw a post by a popular influencer. The post mentioned they would triple anyone's cryptocurrency in one week with their proven method. Tyler was ecstatic and followed the steps to send the cryptocurrency to their account. Tyler waited patiently, but the week went past, and he didn't see his returns or original investment. The influencer later posted that their account had been compromised, and the criminal had posted the message about this cryptocurrency scam. Tyler was embarrassed and chose not to tell his parents or authorities.

Did you spot the red flags?

- The influencer claimed they could triple any investment in one week.
- Tyler was too eager to make quick returns on his investments.
- Tyler's embarrassment after falling for this scam led him to not take any additional action.

This was an example of a **cryptocurrency multiplier scam**. Scammers lure in investors who want faster returns by promising to multiply any deposit made. But more often than not, these deposits go right into the wallet of a scammer with no intention of returning a cent.

These types of scams are very popular on social media platforms. Scammers have been known to **impersonate celebrities, influencers, and popular investors** to push their scams. Additionally, as seen in Tyler's case, real accounts can be compromised and used to push out these scams.



Teach children and teens in your life about the pros and cons that come with investing. Everyone should be aware that scams and other such fraud can, and should, be **reported to local authorities** or consumer protection agencies. It is possible that some, or all, of the stolen money, can be returned.

It's Never Too Early to Train on Cybersecurity

Key Takeaways

Children, teens, and young adults look to us for guidance. Let's set a positive example and teach them about cybersecurity from the get-go! Make sure you are leading by example and follow these recommendations you share.

Set your children up for cybersecurity success by instilling guidance in them as they grow. Share your wisdom and experience on these risks. **No one is too young to be scammed.**

If you've got a child that enjoys gaming, **make sure they know how to play their games securely**. Protect these accounts, keep games updated and monitor for signs of distress from harassing trolls.

Warn your kids about cryptocurrency scams and the potential dangers of investing. **Teach them to avoid get-rich-quick scams**, and that they should speak up if they've been scammed.

Cybersecurity Cryptogram

A Cryptogram takes each letter of the alphabet and replaces it with a number. Using the key at the top, find the appropriate letters that correspond with the phrase below. We gave you a few to start, can you find the hidden phrase below in this month's puzzle?

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
																	8					1		22	

W					Y							W										R	,
1	12	4	20		22	2	9		13	20	2	1		11	4	3	3	4	8				

Y																						R	
22	2	9					16	2						11	4	3	3	4	8				

Answer: When you know better, you do better.