STEALTH FAMILY

PRESENTS

How to Avoid the 7 Newest Cyber Scams and Protect Your Family and Your Fortune From Digital Predators

By Kevin Donahue and Scott Augenbaum (FBI Ret)

Kevin Donahue

Scott Augenbaum

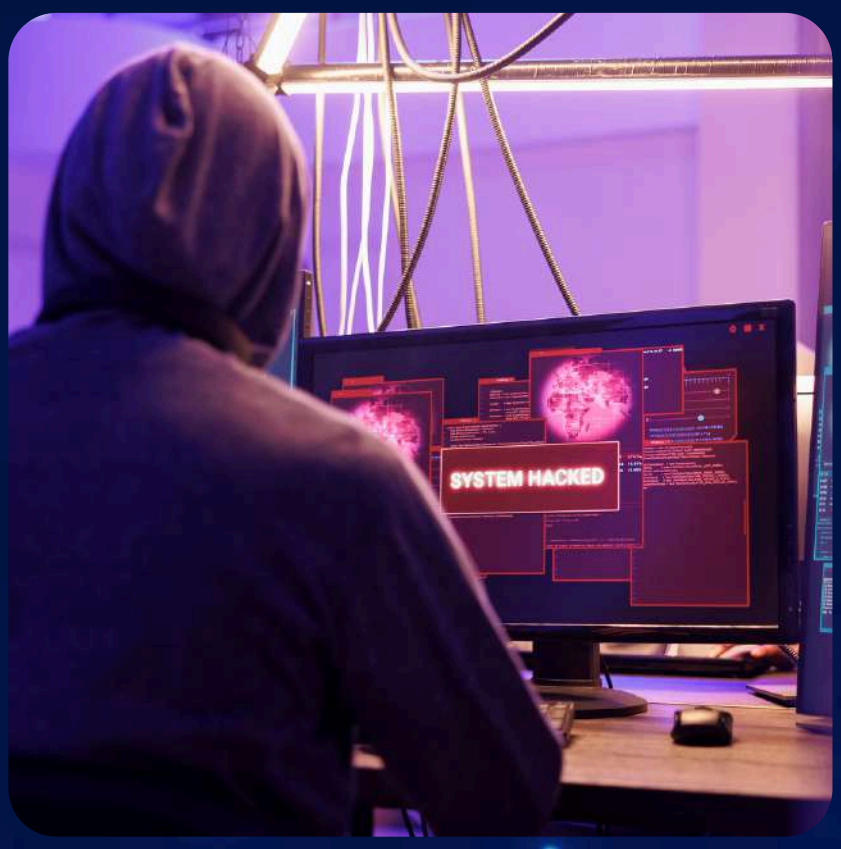
In an increasingly connected world, cybercriminals are continually evolving their tactics to exploit unsuspecting families. These digital predators target both personal and financial information, putting your loved ones and your fortune at risk. Here's a guide on how to avoid the 7 newest cyber scams and protect your family from these growing threats. Be sure to read through to the end where we offer you an opportunity to trial the solution we use in our homes and business. Or you can start now by going to: https://tinyurl.com/4zewd86c

7 Newest Cyber Scams

1. Phishing, Smishing and Quishing Attacks
2. Ransomware
3. Impersonation Scams
4. Online Shopping Scams
5. Tech Support Scams
6. Social Media Scams
7. Online Shopping Scams

1. Phishing, Smishing and Quishing Attacks

Overview:
Phishing attacks remain one of the most common cyber threats, and they're becoming more sophisticated. Cybercriminals send deceptive emails, SMS text messages, or social media posts that appear to be from trusted sources like banks, schools, or even family members, aiming to steal sensitive information. In addition to Phishing and Smishing attacks be aware of QR code phishing attacks as well.



How It Works:

1. A family member receives a seemingly legitimate message asking them to click on a link or provide personal details.

2. The link leads to a fake website that looks real, tricking them into entering sensitive information like passwords or credit card numbers.

3. Once the information is provided, cybercriminals can access your accounts or use your details for identity theft.

Protection Tips:
Educate your family about the dangers of phishing and how to spot suspicious messages. Encourage everyone to verify the authenticity of any unexpected emails or texts by contacting the sender directly. Use multi-factor authentication (MFA) on all important accounts to add an extra layer of security. Never scan a QR code without being sure it is legitimate. When in doubt DO NOT scan. Download our trusted cyber solution suite at https://tinyurl.com/4zewd86c

2. Ransomware

Overview:

Ransomware is a form of malware that can lock your family out of their own devices, demanding a ransom to regain access. This type of attack can be devastating, leading to the loss of precious family photos, important documents, or financial records.

How It Works:

1. Ransomware often spreads through malicious email attachments, infected websites, or compromised software downloads.
2. Once it infects a device, it encrypts files and displays a ransom note demanding payment in exchange for the decryption key.
3. Paying the ransom doesn’t guarantee the recovery of your files, and it may make your family a target for future attacks.

Protection Tips:

Regularly back up important family files to an external hard drive or a secure cloud service.

Ensure all devices in your home have up-to-date antivirus software and avoid downloading files from untrusted sources.

Educate your family about safe online practices, including avoiding suspicious email attachments or links.

Protect your devices by downloading our cyber solution at https://tinyurl.com/4zewd86c

3. Impersonation Scams

Overview:
Impersonation scams involve cybercriminals pretending to be someone you trust, such as a family member, friend, or even a government official. These scams can come through phone calls, emails, or social media, and often involve urgent requests for money or personal information.

How It Works:

1. You or a family member receives a message from someone claiming to be in trouble or needing immediate assistance.
2. The scammer might pose as a grandchild in distress, a family friend needing financial help, or a government official requesting personal details.
3. The urgency and emotional appeal of the message can make it difficult to think clearly, leading victims to comply without verifying.

Protection Tips:
Establish a family code word to verify the identity of someone asking for help in an emergency. In fact, we recommend a family question with answers that don't match the question unique to your family to authenticate the person is real. Encourage your family to always double-check the situation by contacting the person directly through a known phone number or other trusted means. Be cautious about sharing personal information online and limit what you post on social media to avoid giving scammers material they can use. Become a better Digital Parent by trying our cyber solution at: https://tinyurl.com/4zewd86c

4. Online Shopping Scams

Overview:
With more families shopping online, especially during the holidays, scammers are taking advantage of the convenience by setting up fake websites or social media ads that offer products at unbeatable prices. These scams can result in lost money or stolen personal information.

How It Works:

1. Scammers create professional-looking websites or social media ads offering popular products at deep discounts.

2. After you make a purchase, the product either never arrives, or you receive a counterfeit item that doesn't match the description.

3. In some cases, scammers use the payment information to make unauthorized charges or steal your identity.

Protection Tips:
Stick to shopping from reputable and well-known online stores, especially for big-ticket items or holiday gifts. Be wary of deals that seem too good to be true, as they often are. Use secure payment methods, like credit cards or payment services with buyer protection, and monitor your accounts regularly for suspicious activity. Protect your identity and accounts with our cyber solution: https://tinyurl.com/4zewd86c

5. Tech Support Scams

Overview:
Tech support scams prey on families by convincing them that their computers or devices are infected with viruses. Cybercriminals pose as representatives from well-known companies like Microsoft or Apple, offering to fix non-existent problems for a fee.

How It Works:

1. A family member may receive a pop-up message, phone call, or email claiming their device is infected and urging them to contact "tech support."

2. The scammer then asks for remote access to the device, pretending to fix the problem while installing malware or stealing personal information.

3. They may also charge a fee for the "service," adding financial loss to the risk of compromised security.

Protection Tips:
Remind your family that legitimate tech companies will never contact you unsolicited about a virus or security issue.
Never allow remote access to your devices from unknown callers or pop-up messages.
Keep your devices protected with reliable antivirus software and educate your family on how to respond to tech support scams.

6. Social Media Scams

Overview:
Social media is a favorite tool for families to stay connected, but it's also a playground for scammers. These cybercriminals use fake giveaways, quizzes, and hacked accounts to steal personal information or spread malware.

How It Works:

1. Scammers create fake profiles or hack existing ones to post malicious links, fake contests, or quizzes that ask for personal information.
2. Family members may be lured into clicking these links, leading to phishing sites or downloading malware onto their devices.
3. Personal information gathered through quizzes or fake contests can be used for identity theft or further scams.

Protection Tips:
Encourage your family to be cautious about clicking on unfamiliar links or participating in online quizzes that ask for personal details.
Use strong, unique passwords for all social media accounts and enable two-factor authentication (2FA) where possible.
Discuss online safety with children and teens, emphasizing the importance of not oversharing personal information.

7. Cryptocurrency Scams

Overview:
As cryptocurrencies become more mainstream, scammers are finding new ways to exploit people's interest in digital currencies. They may offer fake investment opportunities, fraudulent exchanges, or "get rich quick" schemes that target those less familiar with how cryptocurrencies work.

How It Works:

1. Scammers set up fake websites or social media posts that promise high returns on cryptocurrency investments or offer exclusive mining opportunities.
2. They convince victims to invest money or provide personal information, only for the investment to turn out to be fake or the details to be used for identity theft.
3. The anonymity of cryptocurrency transactions can make it difficult to trace or recover lost funds.

Protection Tips:
Have open discussions with your family, especially teens and young adults, about the risks and rewards of cryptocurrency investments.
Thoroughly research any investment opportunities and only use reputable exchanges and wallets for transactions.
Be skeptical of any offers that guarantee high returns with little risk, as these are often scams.

Conclusion

In the digital age, protecting your family and fortune from cyber scams requires constant vigilance and education and the right tools and resources in place in case something happens. By staying aware of the latest threats and implementing these protective measures, you can significantly reduce the risk of falling victim to digital predators. Make cybersecurity a priority in your home, and ensure that all family members understand their role in keeping your household safe online.

To start your FREE trial of the solution that Scott Augenbaum and Kevin Donahue use and recommend to keep your family safe and to make you a better Digital Parent click here-à
https://tinyurl.com/4zewd86c