



# Protecting Yourself Online

presenter: Special Agent Travis M. Howard

**VALOR • SERVICE • PRIDE**

# My Background

- Joined Virginia State Police in 2007
- Assigned as a Trooper to Hanover/Henrico Counties from 2007-2012
- Assigned as a Trooper to Wise County 2012-2014
- Promoted to Special Agent and assigned to Drug Enforcement Section Wytheville Field Office 2014-2017
- Assigned to High-Tech Crimes Division 2017-Present



# My Background

Primary responsibilities include

- Digital Forensics
- Call Detail Mapping
- Conducting and assisting with investigations with technology element
- Internet Crimes Against Children investigations



# My Background

I have testified multiple times as an expert witness in the field of digital forensics.

Testifying as an expert witness lets you give opinions in court.

Much of this presentation is exactly that, my opinion.



# Note

With technology, there's the rule, the exception to the rule, and the exception to the exception for the rule.

What we'll discuss covers most likely scenarios, but, there will always be a caveat.



# Protecting Yourself Online

What we'll discuss today

- Complex Passwords and Two Factor Authentication
- Ways to protect you from malware
- Common Social Media platforms and how they're used
- Common ways adults and children are abused on those platforms



# Protecting Yourself Online

What we'll discuss today

- Common scams and how to avoid them
- **Red Flags** to look for if you think you're being scammed



# What is Technology?

Technology is a tool

Like any tool, it can be used for good and for bad





VALOR • SERVICE • PRIDE

# Passwords

Why are you required to have Uppercase,  
Lowercase, Number Special Character?



# Passwords

Each small change you make to a password greatly changes its Hash Value

Hash Values are created by algorithms run against each byte of data creating a unique “Digital Fingerprint” of that data.



# Passwords

Hackers maintain extensive collections of password hash values from website and business leaks. Those hash values are used to break your passwords.



# Passwords

Example:

Hello World:B10A8DB164E0754105B7A99BE72E3FE5

H3ll0 W0rld!:BFFB2BDBA2262DAA446173768974AE67



VALOR • SERVICE • PRIDE

# Two Factor Authentication

Two Factor Authentication requires a second method to access your account beyond just entering a password



# Two Factor Authentication

Examples Include:

- Security Questions
- Codes sent to a trusted phone number or email
- Authenticator App



VALOR • SERVICE • PRIDE

# Two Factor Authentication

Two Factor Authentication greatly reduces your risk of having your accounts compromised.



# Ransomware/Malware

High-Tech Crimes Division has seen a tremendous increase in large scale Ransomware/Malware incidents since the start of the pandemic.





# Ransomware/Malware

Incidents have targeted large groups as well as individual users.

Once a computer has been infected and encrypted, little chance remains of recovering important files.




# Ransomware/Malware


Anything you can't live without should be backed up to either cloud based storage or removable storage media.




# Ransomware/Malware

Examples of cloud storage include

- Google Drive 

- Dropbox   
Dropbox

- One Drive 



# Ransomware/Malware

Removable media can be thumb drives, external hard drives, or even DVD's.

If you're using an external hard drive, it should be plugged in just long enough to store you files then unplugged



VALOR • SERVICE • PRIDE

# Ransomware/Malware

Anything plugged into a computer when it gets infected will also be infected.



# Social Media

- There are many different social media platforms in use today.
- We will cover some of the more popular but keep in mind there are many more.



# Facebook



- Largest and Oldest Social Media Platform we will discuss
- Less common for Teens and Children now than in previous years.
- Still heavily used, and can be a hub for scams
- Facebook takes steps to block nudity and report suspected child pornography.



# Facebook

- Common scam involves getting a message on Facebook Messenger from a friend.
- Message will have a link to a video along with a comment of, “I think I saw you here”, or “I think you know this person”
- The link is a virus and can take over your account.





# Facebook



- Facebook Messenger allows for direct chats between the user and their “friends” as well as with strangers.
- Chats can be deleted but are not by default.
- Should be reviewed frequently by parents/guardians



# Facebook



- Facebook is a US based company and will respond to Law Enforcement Records Requests
- If you have been targeted for harassment/abuse or have been victimized on Facebook, Law Enforcement may be able to identify the suspect



# Facebook



- Most importantly, PRESERVE THE EVIDENCE
- Do NOT delete messages
- Do NOT block the account
- This preserves the information needed by Law Enforcement



# Facebook – Best Practices for Children

- Review child's newsfeed to see what they are exposed to.
- Read chat threads frequently
- Attempt to limit use or use Messenger for Kids as an alternative



# Instagram

- Owned by Facebook, now Meta Platforms
- Photo sharing platform
- Has messaging feature



# Instagram

- Shown to be extremely toxic to teens, especially teen girls\*
- Known to cause body shaming issues\*
- Known to cause issues such as depression and self harm\*

\*per leaked internal Facebook documents



# Instagram

- Children, especially teen girls, are targeted on Instagram by strangers for abuse.
- Often solicit nude images which are used again as blackmail or leaked to revenge porn websites.



# Instagram – Best Practices for Children

- Review direct messages
- Review timeline
- Remind children that Instagram is NOT REAL. Images there have been photoshopped and filtered.
- Remind them to NEVER share nude images.





# Reddit



- Described as the “Front Page of the Internet”
- Has unique “subreddits” for almost any interest.
- Does have messaging feature



# Reddit

- Has extensive **NSFW** subreddits
- NSFW = Not Safe For Work AKA pornography
- Children will often meet adults in the NSFW subreddits and then move to a different messaging platform



# Reddit - Best Practices for Children

- Review their Reddit subscriptions and history
- Review messaging history
- Speak honestly with children about the hazards of meeting people that they met online



# Snapchat

- Messaging and social media platform
- Messages go away by default
- Has a hidden folder titled, “My Eyes Only” which is protected by a 4 digit passcode



# Snapchat

- Nude images frequently shared
- Frequently targeted for scams
- Child Predators specifically talk to children on Snapchat because the messages disappear by default
- Some messages are recoverable by Law Enforcement but it is difficult.



# Snapchat Scams

- There is a common scam that involves sharing passwords.
- You get a message from a contact asking for your login info to keep a streak going.
- Once the login info is shared, the account is logged into and the password changed.
- The account is then held hostage and sensitive photos from “My Eyes Only” are taken



# Snapchat Scams

- Those photos are then used to blackmail the account holder.
- Photos will be released to other contacts or posted to revenge porn sites.
- Scammer then uses that account to perpetuate the scam.



# Snapchat - Best Practices for Children

- Don't let children have Snapchat
- Use parental controls and/or parental monitoring software
- Speak to children about not taking or sharing nude images
- Remind children to never share passwords or login information





# TikTok



- Previously known as Music.ly
- Video Sharing Platform
- Has a direct messaging feature
- Filled with Child Sex Predators



# TikTok

- Predators will often pose as children and teens
- Will attempt to gain trust by liking and commenting on shared videos
- Will encourage less clothing in future videos



# TikTok

- Will often manipulate young girls with two main phrases
- “You’re Pretty”
- ”You’re mature for your age”



# TikTok

- Chinese owned company, but has US based offices
- Will accept US based records requests
- Keep in mind, personal data from TikTok is sent to China



# TikTok

- This message came in to an 11 year old's TikTok account after following an account.

🗣️ Hi, I'm live streaming here. Will you come to see me? As long as you come, I will show you what you want to see. One-on-one video with you, I know what a man is thinking. My live room ID:



# TikTok - Best Practices for Children

- Don't let children have TikTok



# Kik



- Messaging Application
- Preferred messaging platform for child sex predators
- Has groups that exist specifically to share child pornography
- Children that meet people of TikTok/Reddit are frequently asked to move to Kik



# Kik

- Historically was not cooperative with US Law Enforcement, which lead to its abuse
- Previously based out of Canada
- Now based out of California and is more cooperative with US Law Enforcement





VALOR • SERVICE • PRIDE

# Kik - Best Practices for Children

If your child has Kik on their phone....

**BURN THE PHONE!**



# Revenge Porn Websites

- Multiple Exist
- Common domain names are .su, .ru
- Usually “based” from a foreign country
- Very rarely can be taken down by US Law Enforcement
- Some underage images may be taken down on a case by case basis



# Online Scams

- Online scams are becoming more common.
- All ages and genders are targeted.
- Scams come in many forms



# Online Scams

- Today we will cover the two most common scams.
  1. Service Scams
  2. Romance Scams



# Service Scams

- Often begin with a call claiming to be your bank, insurance company, or internet provider.
- Sometimes will come from a faked website with fake phone numbers listed. This example is more common with tech related fields (e.g. printer/computer support)



# Service Scams

- If you become suspicious, hang up the phone and call a known number for that institution.
- For Example, You get a call claiming to be from your bank. Hang up and call the number to your local branch.



# Service Scams

- These scams have several common themes that should be **RED FLAGS** when you hear them.
- When you notice these **RED FLAGS**, hang up immediately.



# Refund Repayment

- These start with you getting a refund.
- You are sent “too much” of a refund and have to repay it.
- For example, you are to be refunded \$50, but they give you \$500
- You now need to give them \$450 back.





# Remote Desktop Software

- Remote desktop software has many legal and valid uses but should NEVER be used by your bank, insurance company, internet provider, etc.



# Remote Desktop Software

- Remote Desktop Software allows someone else to completely take over your computer.
- Once they have control of your computer they can install viruses, copy out financial data, and lock up your computer



# Remote Desktop Software

- Examples include:



TeamViewer



CONNECTWISE®



# Remote Desktop Software

- There are dozens of different remote desktop software apps.
- If they give you a new software to download on your computer, do not download it and hang up.



# Gift Cards

- Valid debts and payments are not paid in **GIFT CARDS**
- VALID DEBTS AND PAYMENTS ARE NOT PAID IN **GIFT CARDS**



# Gift Cards

- Examples include
- iTunes Gift Cards
- Google Play Cards
- Prepaid Visa Cards



# Gift Cards

- **Gift Cards** are perfect for gifts but not for paying a debt for service.
- Scammers will have you send them pictures of the cards and numbers
- Once they have that information, your money is gone and Law Enforcement cannot recover it.



# Service Scams

- Use high pressure
- Will claim to be a valid company
- Will ask you to install software on your computer.
- Will ask for payment in Gift Cards.
- Just hang up





# Romance Scams

FTC Data Show Romance Scams Hit Record High; \$547 Million Reported Lost in 2021

New data spotlight shows reported losses up nearly 80 percent from 2020



# Romance Scams

- Romance Scams are becoming an everyday occurrence.
- Can happen on online dating sites and on social media such as Facebook and Instagram.
- Often start as unsolicited messages on Social Media



# Romance Scams

- Will often open up with some variation of “You’re beautiful, I love you”.
- Profile picture is often an attractive man/woman



# Romance Scams

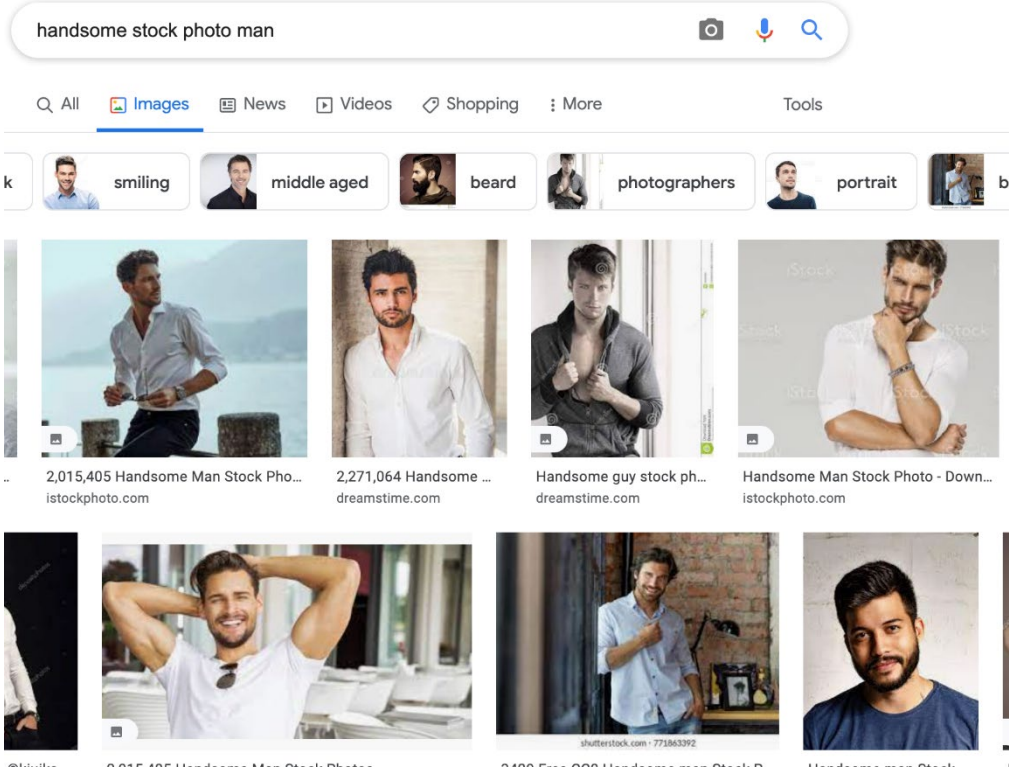
YOU'RE NOT THAT BEAUTIFUL.

STRANGERS ARE NOT IN LOVE WITH YOU.

THEY ARE IN LOVE WITH YOUR RETIREMENT SAVINGS.



# Romance Scams



# Romance Scams

- Scammers will use stolen or stock images of beautiful people as their profile picture.
- You can search that image on the internet to see if it's real.



# Romance Scams

- May take place over an extended period of time.
- Main difference from traditional scams is that the request for money is not always immediate.



# Romance Scams

- Scammer will take their time in an attempt to build trust.
- May not even be a direct request for money.





# Romance Scams

- “I’m behind on my rent and they’re about to kick me out”
- “I’m stuck overseas and can’t afford a plane ticket to get to you”
- “I was on my way to you when my car broke down”



# Romance Scams

- May request money in gift cards or request to mail cash.
- Cash may be sent to someone else that they are scamming.



VALOR • SERVICE • PRIDE

# Romance Scams

Just like with other scams, the money is almost never recovered by Law Enforcement



# Conclusion

- Use strong passwords and Two Factor Authentication
- Store important files in either cloud storage or removable drives
- Don't click on suspicious links sent to you on social media
- Monitor social media use of children



# Conclusion

- Consider banning children from certain social media platforms
- Look out for **RED FLAGS** if you think you're being scammed
- Strangers on the internet are not in love with you.



VALOR • SERVICE • PRIDE

# Contact

Special Agent Travis M. Howard  
1186 E Lee Highway  
Wytheville, VA 24382  
[Travis.howard@vsp.virginia.gov](mailto:Travis.howard@vsp.virginia.gov)  
(276)613-3301

