Online Safety Event 2020 Script

Slide 1 – Title

Welcome, thank you for coming and introduce self

Why are we here today?

- AT&T and Oasis are here to share information about internet safety!
- It's our goal that you leave here today with the ability to identify when you're being targeted and understand how you can be proactive about protecting yourself online. We want to take away the fear or embarrassment you may feel around these issues and empower you with best-in-class resources.

Slide 2 – Agenda

Here is what we are going to talk about today:

1: Who is more vulnerable to scams?

2: How to fight back against scam tactics

3: Tips to stay safe online everyday

4: How AT&T and Oasis can help you

Slide 3

Who is more vulnerable to scams?

Slide 4

There are three primary factors that make older adults more vulnerable to frauds and scams.

a. First, according to a report by AARP, older adults hold the vast majority of wealth in the United States. Many older adults have retirement savings, paid off mortgages and pensions. If an older adult falls prey to a scammer they often have more money to lose than a younger person does.

Slide 5

b. The second complicating factor for older adults: There are variety of scams that are designed just for older adults including Social Security scam, Grandparent scam, Funeral/Cemetery, Medicare scams, Reverse mortgage or homeowner scams and fraudulent anti-aging products marketed to older adults.

Slide 6

c. The third complicating factor for older adults: Research from Cornell University and the Federal Reserve Bank of Chicago shows that older adults experience brain changes that can alter the ability to make sound financial decisions. Additionally, older adults often experience social isolation and being isolated from others makes people more vulnerable to exploitation. Having a trusted person who you can discuss financial decisions with is very important.

Questions?

Slide 7 – FBI data by age

According to the 2019 FBI Internet Crime Report

a. Everyone is experiencing scams online. But when older adults fall victim, reports, like the FBI's report, show they lose more money than others. The purple, 2019 Victims by Age Group, shows people over 50 lost about $1.4 billion dollars in 2019 to cybercrime. Also, note the sharp increase in money lost to people under 20.

Slide 8 – FBI data by crime type

b. BEC/EAC (Business Email Compromise or Email Account Compromise) are sophisticated scams targeting both businesses and individuals performing wire transfer payments. The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.
c. According to the FBI, this is the number 1 crime by total numbers lost by victims. By a lot. The green, 2018 Crime Type chart, show other common cybercrimes and show how dangerous all can be if you don't protect yourself online.
d. For older adults: Romance scams, Government impersonation scams, Tech support scams (up by 40% in one year) and Charity scams continue to be the most harmful to older adults.

Questions?

Slide 9

AT&T research

a. According to a new survey, commissioned by AT&T, **95% of older Americans (aged 60 years or older) have experienced a scam online.** More specifically, the survey found:
b. **92% of older Americans** have experienced some sort of phishing attempt.
c. **71% of older Americans** have encountered a malicious actor claiming to be someone else. (That can mean collection agent, company shutting down service, support technician, family member in trouble, etc.)

Slide 11

Now we are going to share three kinds of common scams and how you can protect yourself

Slide 12

How scammers lure victims on the internet

Posing as someone they are not (**Play the entire video** Catfishing and romance scams**)**

i. Be wary of unexpected invitations to connect from total strangers, especially if the profile picture is very attractive, the person lives a long distance for you or is not within your age group.
ii. If your new acquaintance seems to have a lot in common with you, think twice. This is how catfishers build an emotional relationship with you.
iii. If the new friend can never meet, talk live on the phone or have a video conference with you, that's a red flag.

Questions?

Slide 13

Demanding payment with gift cards **Play the entire video**

Slide 14

i. Gift cards are for gifts PERIOD and you should be skeptical of anyone who requests payment by gift card may not be legitimate—
ii. Most common requests for gift card payment computer tech support, the IRS, the police or a utility company.
iii. Scams like these try to:
    i. Play on your emotions
    ii. Make you think something is really important.
    iii. Try to convince you that they are going to help you from causing a tragedy

Questions?

Slide 15

Charity frauds and scams

Slide 16

Make sure the charity calling or emailing you is legitimate

i. Look at its website and social media
ii. Research ratings on
    a) Charity Navigator
    b) Guidestar

c) BBB Wise Giving Alliance

iii. Volunteer for the charity to learn more about it

Questions?

Slide 17 – now I'd like to share some general tips

Slide 18

5 Key Tips for being safe online everyday (these are the tips on your post-it note pads that we are giving away today – please share with friends!)

a. The best way to protect personal information is to be aware of where you are giving it away and then change your behavior.
    a. If your phone is not locked with a passcode, fingerprint or facial recognition all the information in your phone could be accessed if your phone is stolen.
    b. People also share a lot of personal information on social media sites like Facebook and Instagram.
b. Look at all emails carefully to make sure they are really from the person or organization they claim to be.

c. If an email has an attachment or a link inside it you want to be very careful and assess that the link or the attachment do not install a virus or malware OR take you to a site that will collect more of your personal information.

d. Password managers create passwords and alert you when passwords are weak or have been compromised.

    a. Long and strong (when possible).

    b. Mix of upper and lowercase letters, numbers and symbols.

    c. No sharing!

    d. Make your password unique to your life and not something that is easily guessed

    e. Have a different password for each online account.

    f. If you write down your password, store it in a safe place away from your computer.

    g. Change your password several times a year.

If you prefer not to use a password manager you may use a password generator—Generate random passwords with a password generator (State of Missouri offers one here: https://cybersecurity.mo.gov/tools/password_gen/

e. Login to financial accounts regularly to verify that balances are correct. Consider setting up two factor authentication so that no one can login without a second layer of protection provided by a text message received on your phone. Consider setting up text alerts so you know when activity is posting your account.

Slide 19

Lock your phone **(Play at least the first minute of this video)**

Slide 20

i. Set a passcode or PIN to prevent a criminal from getting access to private information stored on your device. Some smartphones offer fingerprint or facial recognition, but it all starts with a passcode.
ii. Create a lock screen message asking the finder to call or email you if the phone is found.
iii. Set up your device to use the finder apps to locate your lost device and secure or erase your device remotely.
    1. On an iPhone, go to Settings and turn on Find my iPhone.
    2. On an Android, go to Settings and turn on Find my Device.

Slide 21

Limit the personal information you share on social media, video calls, phone calls or or email. If you don't know the person asking you for information or help, they may be scam artists. As a general rule, no legitimate company will ask for financial, sensitive information directly in an email. They will require you to sign into account on a secure website first.

Slide 22

i. Social media is not necessarily private. Even if you share a message or photo with someone privately, you lose control as soon as it's in someone else's hands. Assume that everything you share on social media has the potential to be public. This includes sharing your whereabout and when you are out of town.
ii. Not all social media contacts are genuine. Anyone can create a social media account and call themselves by any name. Scammers often clone existing real accounts in order to get personal information.
iii. Think twice before you participate in social media surveys. They can seem harmless, but they can be a way for scammers to initiate a conversation with you. Make sure you are confident of the source of the survey before you fill it out.

Questions?

Slide 23

Report all scams and frauds to the government. There are three websites and one phone number where you can officially report a scam. You can take a picture of this slide if you prefer

Slide 24 How AT&T and Oasis can help you

Slide 25

AT&T has created two great apps for you. The first is AT&T Mobile Security which you can download from the App store or Google Playstore. Both apps have free features

a. Mobile Security is available in Android and

Slide 26 iOS

i. AT&T mobile Security has different security features to protect your phone depending on what kind of phone you have.

ii. AT&T Call Protect features are

1. Automatic Fraud Blocking
2. Warnings of Spam and other nuisance calls
3. Personal Block List to block calls

Slide 27

iii. AT&T Mobile Security are:

1. Device Security
2. Breach Reports

b. Both apps have additional features that you have to pay for.

Slide 28

Connect with someone you can trust—

c. an accountability buddy/someone you can trust to ask:

i. Does this sound right to you?

ii. What's the worst thing that can happen if I don't take this action?

d. Who can you talk to?

i. Your state's elder abuse hotline https://elderprotectioncenter.com/state-elder-abuse-hotlines/

ii. Oasis employees

e. Share this information with your friends and family

f. Visit these webpages for updated information

i. Connections.oasisnet.org/safety

ii. Cyberaware

Slide 29

Thank you!!!!