




PWC G8
Gals@Technology

Scams: Old and New

April 18, 2022





1

Scott Ksander

ksander@purdue.edu



- 40+ years in the IT field, 26 years at Purdue
- Wrote his first program (FORTRAN) when he was in 5th grade. Purdue degree in Computer Science.
- Areas of interest – systems development, networking, security
- In retirement, Scott writes a technology column for the Purdue Retirees Newsletter and does presentations for the Purdue Women’s Club
- Scott and Peggy enjoy life with their kids and grandkids – especially on trips to DisneyWorld
- Scott grew up in Chicago and Peggy grew up in Fish Lake, Indiana (city boy meets farm girl at Purdue story – and the adventure continues ...)

2

Current Topics – Cyber Warfare

- “Senior U.S. law enforcement and Homeland Security officials have told ABC News that there is growing concern that Russia could launch further cyberattacks against the West. The potential targets include electrical grids, banking systems and mobile networks, according to the officials.”
- "Freaking out is not a productive thing to do. There are lots of reasons to think that the fact that something is out there but that doesn't mean it could happen," Stuart Madnick, the founding director of Cybersecurity at MIT Sloan, told ABC News. "But there are still a number of things that people can do to stay safe and protected."
- There are two types of cyberattacks, he said: ones that have an indirect impact on people's livelihood and attacks targeting the tech of specific people.

The biggest indirect hacking examples in the past have targeted key infrastructure points such as the Colonial Pipeline ransomware attack in May 2021, which affected everything from gas prices to flights.

"In the last two years, we've been seeing more of these attacks around the world," Madnick said. "You need to realize how many of our systems are connected to computers and just one hack can have bigger effects."

- The federal government has called on businesses to make sure their information technology teams update their computer software to close any vulnerabilities and train their employees to watch out for any malware.

3

Current Topics – Cyber Warfare

- Mandate the use of multi-factor authentication on your systems to make it harder for attackers to get onto your system;
- Deploy modern security tools on your computers and devices to continuously look for and mitigate threats;
- Check with your cybersecurity professionals to make sure that your systems are patched and protected against all known vulnerabilities, and change passwords across your networks so that previously stolen credentials are useless to malicious actors;
- Back up your data and ensure you have offline backups beyond the reach of malicious actors;
- Run exercises and drill your emergency plans so that you are prepared to respond quickly to minimize the impact of any attack;
- Encrypt your data so it cannot be used if it is stolen;
- Educate your employees to common tactics that attackers will use over email or through websites, and encourage them to report if their computers or phones have shown unusual behavior, such as unusual crashes or operating very slowly; and
- Engage proactively with your local FBI field office or CISA Regional Office to establish relationships in advance of any cyber incidents. Please encourage your IT and Security leadership to visit the websites of [CISA](#) and the [FBI](#) where they will find technical information and other useful resources.

4

We Grew Up In a Different Time



5

We Grew Up In a Different Time

- ▶ Average cost of a new car - \$1,700 (1952)
- ▶ Dozen eggs - 25 cents
- ▶ Gallon of gas - 20 cents
- ▶ Average college professor salary - \$5,100/yr
- ▶ Life was more local
- ▶ Long distance communication was expensive
- ▶ We were more trusting

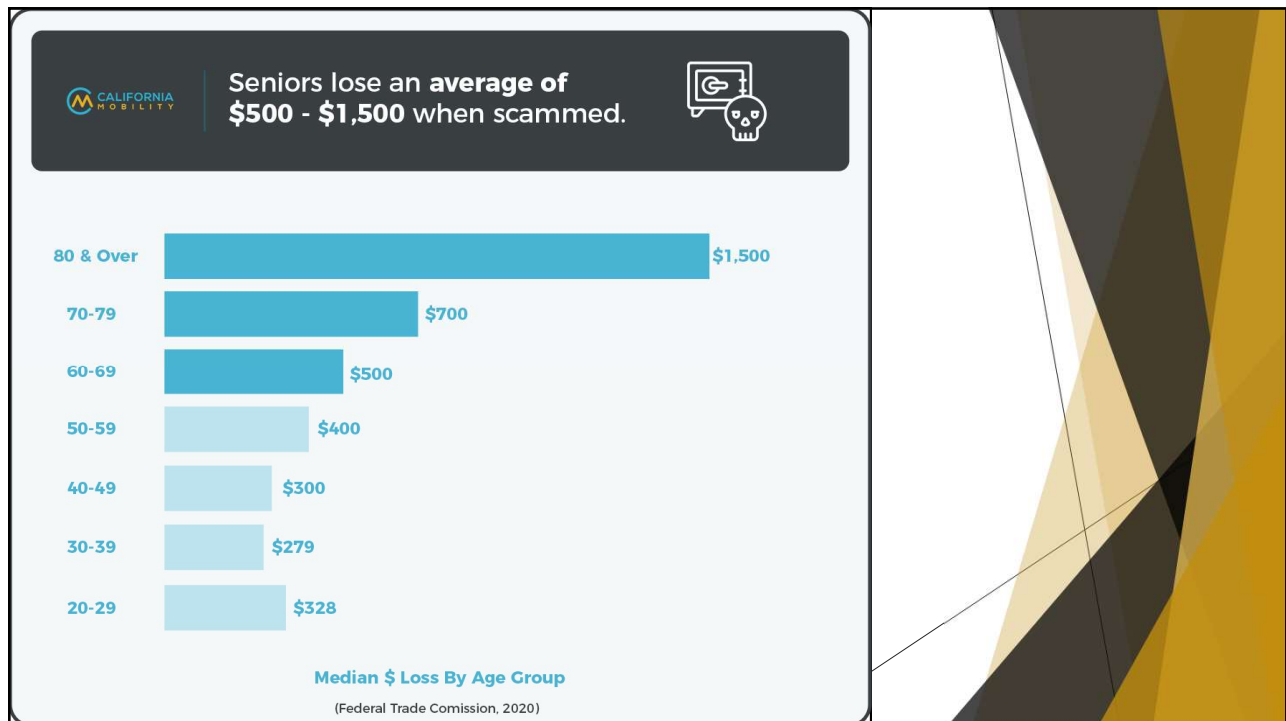
6

We Are The Target

- ▶ Seniors tend to be trusting and polite
- ▶ Seniors usually have financial savings and good credit
- ▶ Seniors are less inclined to report fraud

- ▶ “Elder fraud” currently nets \$3 Billion annually and growing

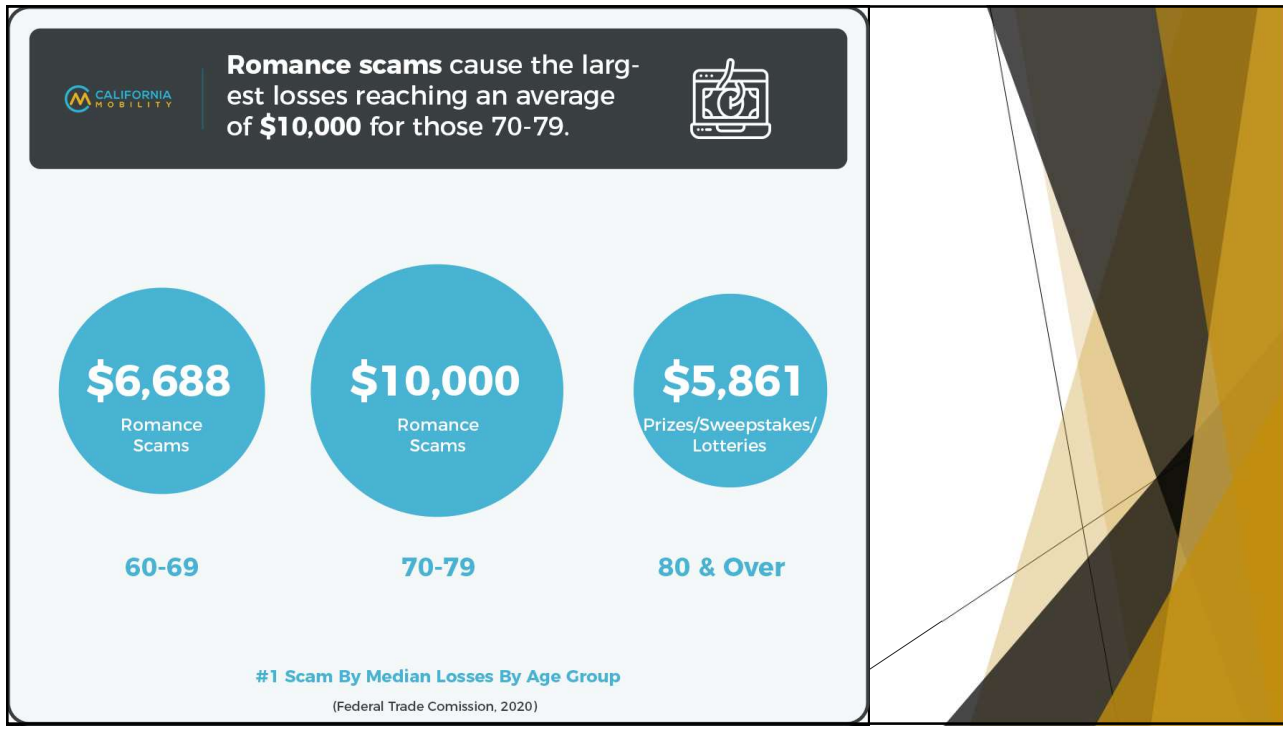
7



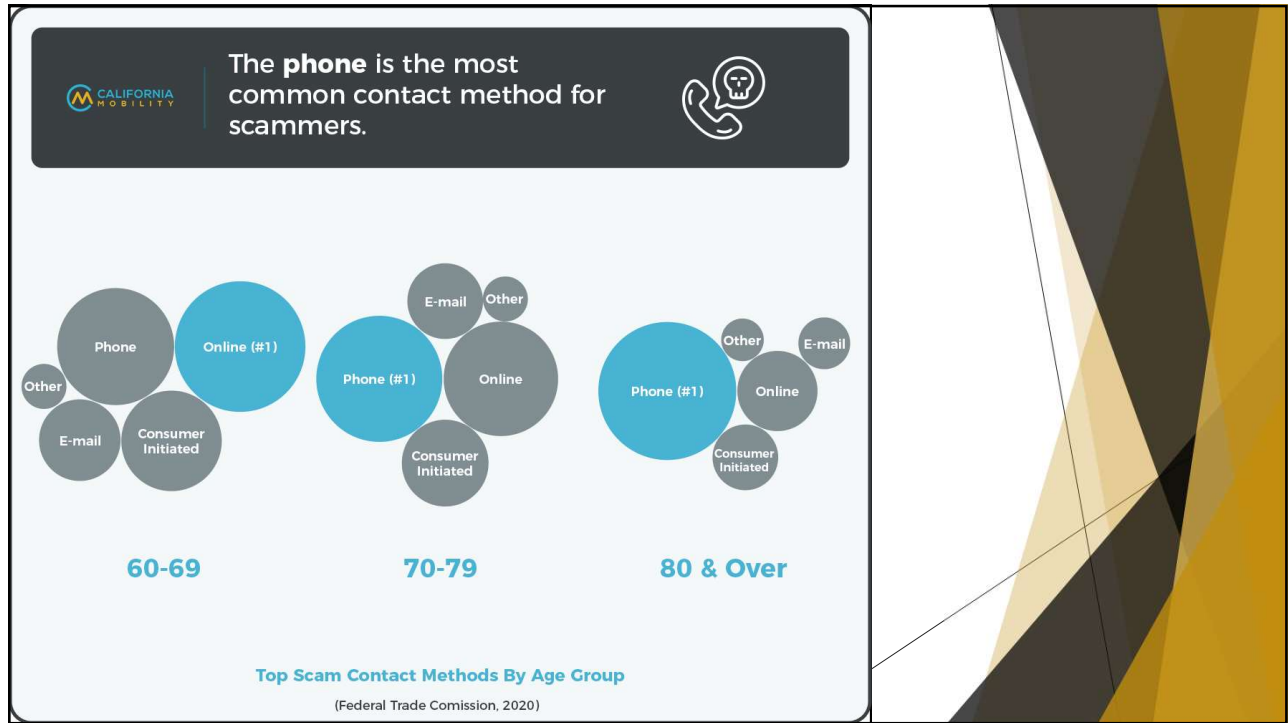
8



9



10



11

Golden Rules

- ▶ Slow It Down! Panic is their objective.
- ▶ Do your research and double check.
- ▶ Stop! Don't Send.

12

Things That Will NEVER Happen

- ▶ Microsoft will NEVER call you
- ▶ Amazon will NEVER call you
- ▶ The IRS will NEVER call you
- ▶ Apple will NEVER call you
- ▶ Nobody is monitoring your PC or phone to call you and “help” with problems

13

Common Types of Scams

- ▶ Sweepstakes/Charity/Lottery scams
- ▶ Romance scams
- ▶ Grandparent scams
- ▶ Fake Medical Insurance Plans
- ▶ Tech Support scams
- ▶ Robocall Credit Card Interest Reduction
- ▶ Business Opportunity Schemes
- ▶ Money Transfer Systems Fraud
- ▶ Real Estate Scams

14

The Objective - Your Identity and Your Money

- ▶ The more I can learn about you, the easier it is to impersonate you
- ▶ Get you to panic and disclose information or send money
- ▶ Get you to click on an unknown website so they can gather your information

15

Phishing Email


- ▶ Think before you click

“To improve your credit score, just click [HERE](#)”

To stop getting these annoying emails, just click [HERE](#)”

16

Your PAYMENT !! (URGENT)

 BBVA Bank <tx@bbvaus.com>
To: ksander@purdue.edu

BBVA Bank
Address: 2001 Kirby Dr, Houston, TX 77019, USA
Tel: +1 (713) 831-5808 : Direct Line: +1 (713) 987-4282

Working Hours:
Monday - Friday 8AM-6PM
Saturday - Sunday Closed

REF: BBVAUSA/GOV/RF/GRANT/5M/050920

Dear Sir!

You have a payment of Five Million USD (\$5,000,000) with us at BBVA Bank - River Oaks; # 2001 Kirby Dr, Houston, TX 77019, USA

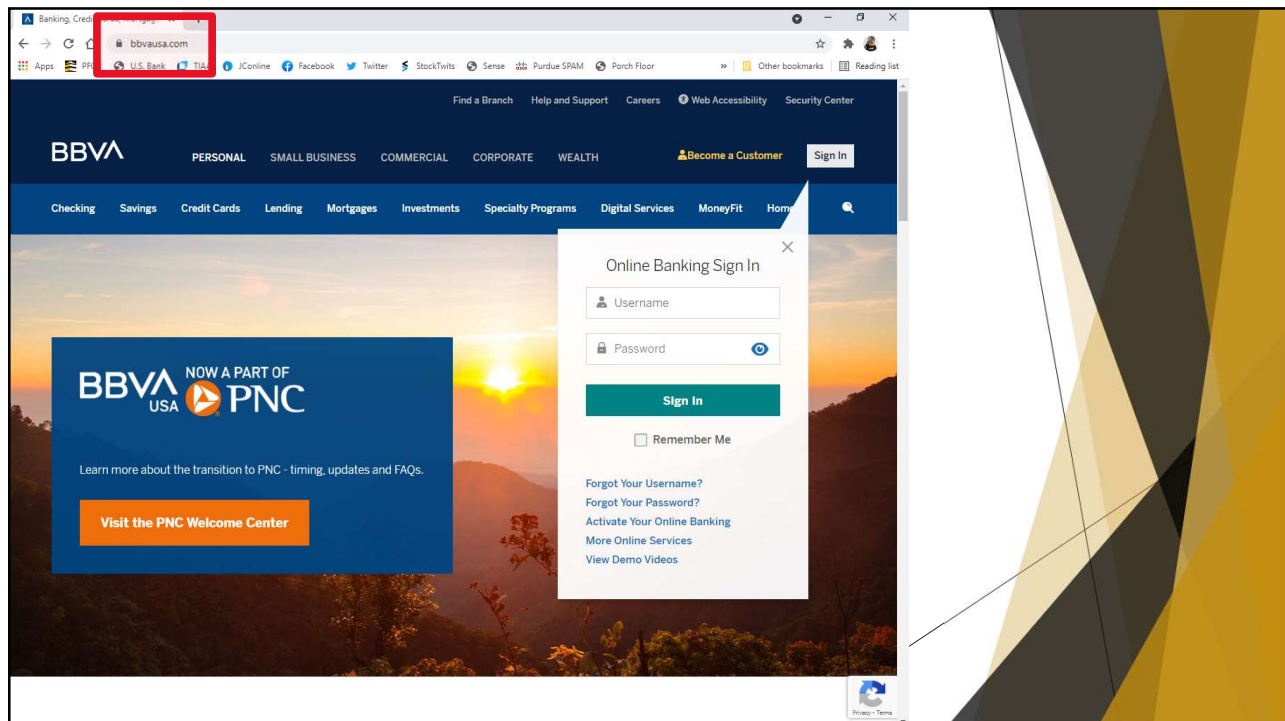
Your name and email address was submitted to our bank by your State Government as one of the Government recipients to receive the State Government COVID-19 Financial Aid (Economic Relief Grants).

Please email this office with a Copy of your ID card (Passport or Driving License), Your full Names, Address, Profession, Phone/WhatsApp Numbers, to enable us to process the transfer of your fund before the bank closes today as instructed by your State Government.

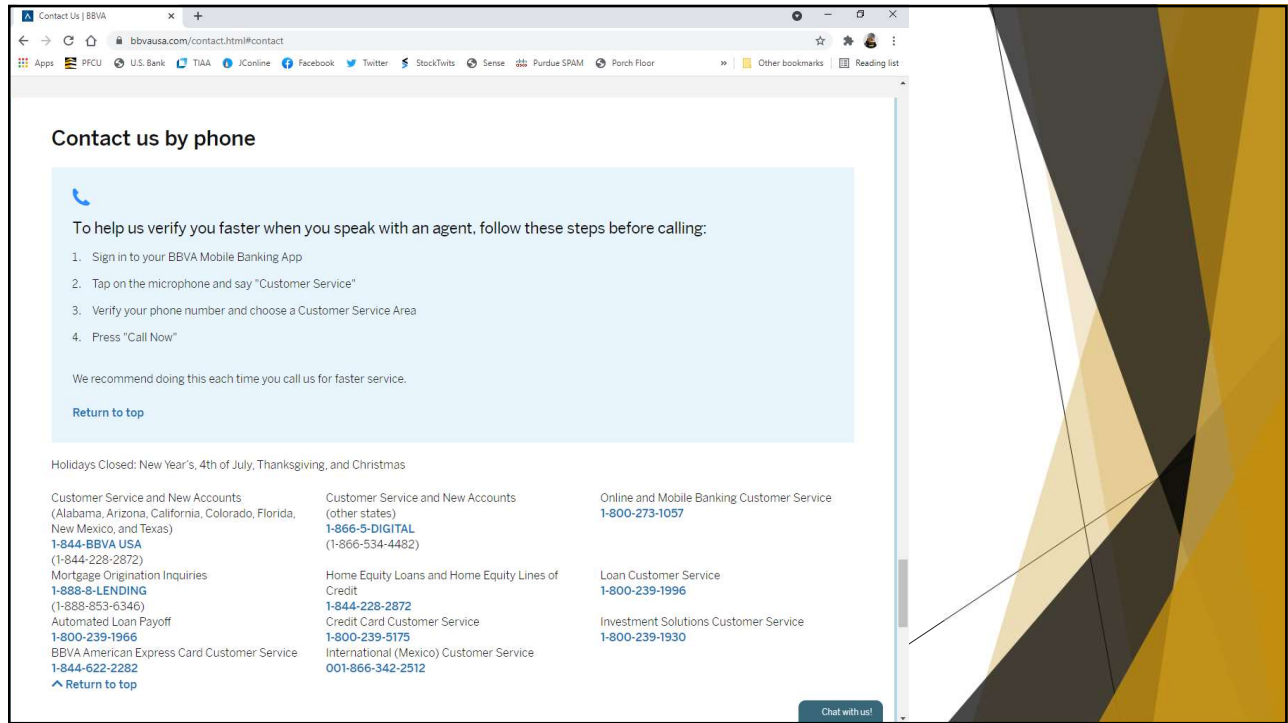
Our team is available via WhatsApp as an alternative to email should this be a preference.

Sincerely,
Chris STEPHENS (Dr.)
Director of Operations BBVA USA
e-Mail: dr.cstephens@usbbva.us

17



18



19



20

Fake Phone Calls (Caller ID is VERY easy to fake)

“I am researching COVID-19 vaccination opinions, can you please read me the information on your vaccine card.”

“I need to confirm your vaccine information for our records so you can get a refund on your 2022 income tax.”

21

Top 7 scam predictions for 2022

#7: COUNTERFEIT SHOPPING SITES. ...

#6: NATURAL DISASTER SCAMS. ...

#5: CRYPTOCURRENCY CONS. ...

#4: DATA BREACHES. ...

#3: SOCIAL ENGINEERING SCAMS. ...

#2: THE INTERNET OF THINGS. ...

#1: SIM SWAPPING. ...

22

SIM Swap Scam

- ▶ The fraud exploits a mobile phone service provider's ability to seamlessly port a phone number to a device containing a different subscriber identity module (SIM). This mobile number portability feature is normally used when a phone is lost or stolen, or a customer is switching service to a new phone.
- ▶ The fraudster contacts the victim's mobile telephone provider. The fraudster uses social engineering techniques to convince the telephone company to port the victim's phone number to the fraudster's SIM. This is done, for example, by impersonating the victim using personal details to appear authentic and claiming that they have lost their phone.
- ▶ Once this happens, the victim's phone will lose connection to the network, and the fraudster will receive all the SMS and voice calls intended for the victim. This allows the fraudster to intercept any one-time passwords sent via text or telephone calls sent to the victim and thus allows them to circumvent many two-factor authentication methods of accounts (bank accounts, social media accounts, etc.) that rely on text messages or telephone calls.

23

What Can We Do?

- ▶ Slow things down and don't panic
- ▶ Never give out personal information
- ▶ Research with others. Re-contact people at a number or address you can verify.
- ▶ Don't accept contacts (email or phone) from people you don't know. Verify that they are people you know. (challenge question)
- ▶ National Elder Fraud Hotline 1-833-372-8311 (1-833-FRAUD-11)
- ▶ FTC - 1-877-382-4357 (1-877-FTC-HELP)

24



25