Covid-Scams Timeline

March 2020

- **Fake websites** for in-demand items such as PPE and masks
- False advertising, **price gouging**, miracle cures
- Con Artists **impersonated the CDC and WHO in phishing emails**
- Donating to **fake government fundraising efforts** to develop a Covid vaccine
- Telecommuting. Scammers and hackers capitalized on new work-from-home workers. Zoom bombing took place in video conferences.

Late March - late May 2020

- **Round 1 of stimulus check scams**. Government imposters called about the checks and scammers conned victims into thinking they qualified for a special Covid-19 grant. These grants claimed they helped pay medical bills or just provide funds, some upwards of $150k. Scammers used an official looking website to phish for personal information, social security numbers and banking information. Some phishing sites had a small "processing fee" attached.

- Scammers sent text messages, **impersonating the US Dept of Health & Human Services, mandating people to take an online Covid-19 test**. A link was included in the text. There was no such test.

- New work-from-home employees found themselves more **vulnerable to tech scams through fake-pop ups, virus alerts and Business Email Compromise scams**.

- Employment scams – scammers capitalized on **"work from home" opportunities**. Not all opportunities were legitimate.

- **Phony SBA Grant Offers and predatory lending was hot** – enticing interest rates encouraged businesses to refinance. BBB warned about researching lenders.

- Facebook Quizzes were a norm to see in facebook feeds, seeking people to **post personal information** about themselves.

June 2020

- Consumers were receiving **contract tracing scam calls**, advising them they came in contact with someone who tested positive for Covid. Asked you to **click on a link where malware was downloaded to your device**. Scammers also called asking to **verify personal information including your full-name, DOB and other personal and financial information such as bank accounts**.

August 2020

- Scams promising free money from government aid programs, and SBA imposter scams. "Consultants" reached out to consumers and said they could **get aid from unadvertised programs or programs where your application was previously denied**. There was typically a fee associated with this service. Victims paid it and never heard back from the "consultant."

November 2020

- **Online puppy scams**. People were working from home and had more time to devote to a new family member. BBB received nearly **4,000 reports with a median loss of $750 and $3 million total lost** from this scam. Those numbers are 5x more than the period from 2017 – 2020.

December 2020

- The Covid vaccine was on the way, along with the scams. **Phony Covid testing kits, treatments and fake vaccines were in the headlines**. Scammers used **phishing messages to trick consumers to share passwords and personal information**.
- Robocalls impersonating government officials increased.

Early 2021

- **Stimulus check scams** surrounding another stimulus payment
- BBB urged **not to share your vaccine card to social media**. Posting gives scammers the opportunity to take this info, including your name, date of birth, vaccine brand, lot number and date of vaccine and scam you during a future attempt – possibly identity theft. Or, scammers can take your card, recreate it and sell a phony version.
- **Fake unemployment claims**. Scammers took advantage of increased unemployment to collect benefits in the names of unsuspecting victims. Tactics used included phishing for social security numbers and other information by sending fake notifications from financial institutions and government agencies. Cold calls to potential victims were also made to coax them into sharing personal information.

What's going on now? March 2021

- Scammers have taken advantage of the demand for vaccine appointments. **"Vaccine Hunter" sites** are popular to help consumers find open appointments and leftover doses in the area. While many of these sites are legitimate, the situation is an ideal opportunity for scammers to **promote look-alike websites that collect personal information or require payment**. BBB warns consumers to use caution when following links and providing personal information.