What to do if you've been scammed.*

1. Don't be embarrassed it happens to the best of us, be sure to talk to loved ones ASAP.

2. Call the bank and any other money service in your name and get them locked down.

3. Contact the three credit major credit bureaus, alert them to the problem. This will help prevent the thieves from opening new lines of credit in your name.

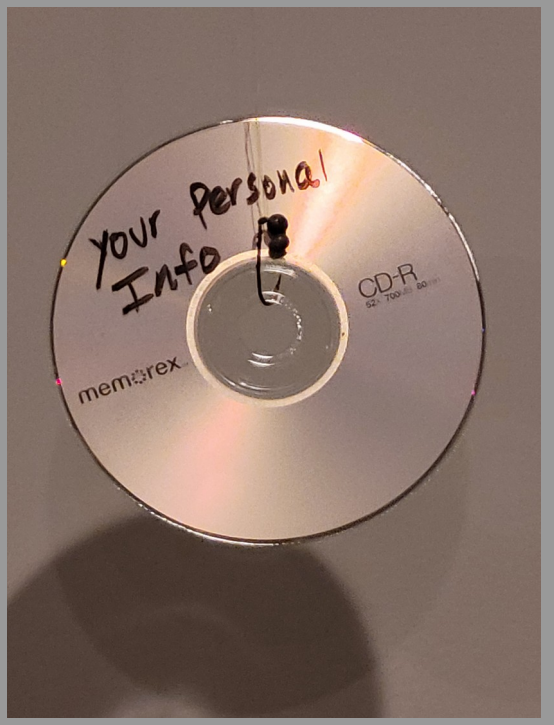
4. Change all electronic passwords. Any website you use frequently, change the password.

5. Report the crime, make sure to alert the local police and any state, FBI or other federal agency as directed.

Stay safe out there, don't let the scammers get your hard earned money. Make sure and share this with others you know.

*McGreevy. (2019, July 30). The Penny Hoarder. The Penny Hoarder. Retrieved April 2, 2022, from https://www.thepennyhoarder.com/save-money/fraud-scam-victim/

All pictures are from creator of the brochure, Jordan Ferguson



Avoid Being Phished

By Jordan Ferguson

What is Phishing?

Phishing is when someone is trying to trick you into giving them your information through a fraudulent email, text, or fake website that looks like a trusted website.

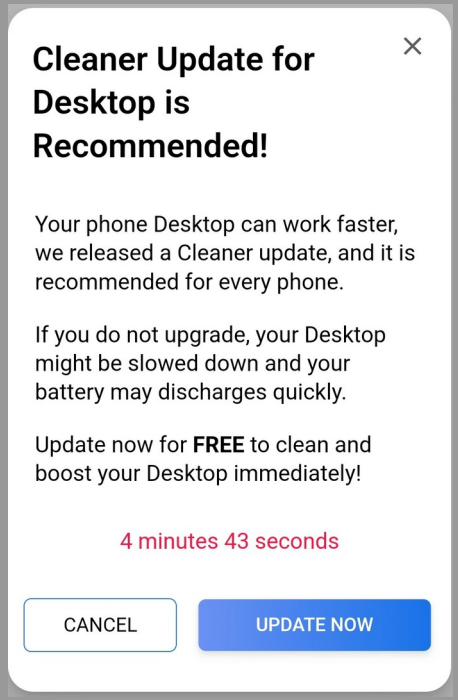
Common signs to watch out for to catch a phishing scammer.

Phishing emails and websites will try to make you feel like it is something urgent, with words like “your required to update your information now on our website to continue using our service.” Misspelling is intentional for this example, many phishing messages are riddled with spelling errors.

Phishers will also try to force you to their websites or send attachments that are virus laden to steal your information.

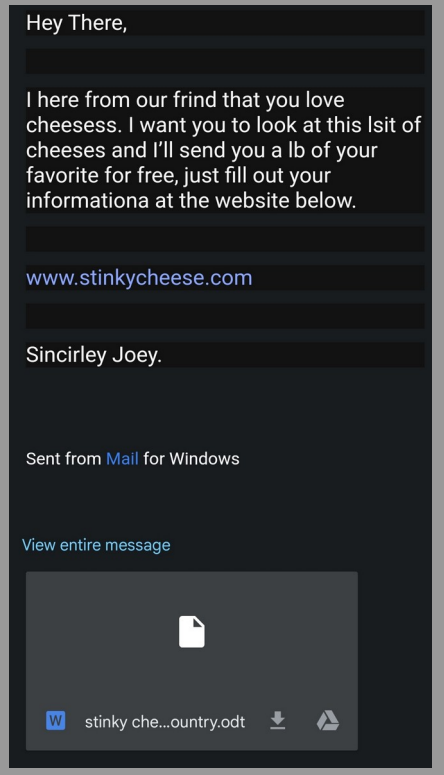
Another easy tell that it is a phishing scam, is the promise is too good to be true, such as a large return on an investment or free money for simply filling out a form.

By playing on our base emotions of anger, greed and fear, scammers will try to make you feel like you are in a desperate or amazing situation, depending on what they feel will help them get your info and money.



What to do if you see a phishing scam.

1. DO NOT OPEN ANY ATTACHMENTS FROM PEOPLE YOU DON’T KNOW.



2. If you suspect something is amiss, delete the message. Block the sender.
3. Make sure to pass on the information of what you saw to your loved ones so that they aren’t tricked either.