



Current Fraud attempts

Periodically Pioneer Bank & Trust will post information on the types of fraudulent communications our customers may be seeing. This is not intended to be a complete list of fraudulent communications you may receive but rather an update of the types of fraud we are seeing the most.

Smishing - smart phone users are subjected to text-based phishing attacks for account credentials.

If you receive a text asking for account credentials or any type of personal information, please do not respond to the text. Pioneer Bank & Trust will NEVER ask for your information with a text and most reputable companies have a similar practice.

Malware - Software that is put on your computer or phone that will forward information to the person(s) who created and distributed the software allowing them to receive your personal information.

While this type of threat has been in existence for quite a while, there is an increase in the number of malware infections. In part the increase is attributable to social media (Facebook, Twitter, etc.) where users seem more willing to click on links that automatically install the software.

The best defense against this threat is to have anti-malware software installed and kept current. You should also use caution when you are online and ask yourself if the information you are seeing makes sense. Some ways the malware has been distributed includes a scare tactic where you are told you have an infection on your computer and to click a link to remove it. If the notice is not from the anti-malware or anti-virus software you have installed on your computer, do not click on the link as most likely it will install malware on your computer or phone.

Another method being used is to broadcast emails with the hope that you will click on links put into the email. We have seen emails that seem to be from the IRS, ACH processing organizations, and financial institutions. Again a scare tactic may be used that tells you there is a problem with a payment or another tactic is to tell you have money due to you and only have to click the link to receive it. Ask yourself how your email address is known by whoever the email is supposedly from. For example, if the email indicates it is from the IRS but you have never given the IRS your email address how would they have known your email address? If it does not make sense, do not click on any of the links and even better, do not open the email.

Polymorphic malware - is a form of malware that is constantly changing the way it looks to anti-malware software making it difficult to identify it as malware.

This is the newest form of malware and is making it difficult for the software companies to be able to identify and remove it once it is on your computer. Your best defense is to use the precautions identified in the malware section to never have the malware on your computer.

Most threats can be avoided by applying some of the common sense tactics explained here but occasionally your computer or phone may be infected with a threat despite your best efforts. Some of the tell tale signs include:

- Popup windows that you did not expect
- Your internet is slower than it has been
- Your computer is slower than it was
- Unexpected icons on your desktop
- Unexpected items in your browsers bookmarks or favorites
- Unknown items in the system tray of your computer
- Unknown programs on your Add/Remove programs list

Become familiar with these areas on your computer so you can identify when changes are made. If you think that something just is not right, run the software you have installed on your computer to check for viruses and malware. If you are not sure about some item show in one of the areas on the list above, search the software company you use for these protective services to see if they have identified any issues with the item. If you find nothing there, search the internet for the item you are not sure about.

If you still suspect something just is not right, disconnect your computer from the internet and consult a professional.

Pioneer Bank & Trust