CITY OF PARMA OHIO

LAW DEPARTMENT

6611 RIDGE ROAD | PARMA, OHIO 44129-5593 | 440-885-8132

Timothy G. Dobeck
Law Director
Prosecutor

February 9, 2018

LAW DIRECTOR ADVISORY

Phishing Scams

It has come to the attention of the City of Parma Law Director's office that Parma residents are once again at risk of becoming victims of a scam. A Parma resident noted that her bank informed her that a "phisher" called the bank attempting to get information about the resident's bank account. On the same day, the resident also received a phone call, which the resident believed to be a scam and connected to the "phishing" attempt. Once the resident was notified about the scam, she notified the Federal Trade Commission ("FTC") and the City.

Phishing is a form of scam where the phisher will target an individual by posing as a legitimate institution to lure individuals into providing valuable data, such as personally identifiable information, banking and credit card details, and password. Once this information is gathered, the phisher uses it to access important accounts, which can result in identity theft and financial loss. Phishers will attempt to gather your information by any means necessary. This means a phisher will attempt to communicate with you by phone, e-mail or by computer virus.

The Parma Law Director's office encourages Parma residents to report any suspicious behavior. Do not trust unfamiliar or unidentified callers. You should never provide or confirm sensitive information over the phone. Should you believe the service to be legitimate, ask for a call-back number, and conduct research to ensure it is not a scam. One step you can take to ensure the call is legitimate is to look up a customer service number for the service and inquire as to the legitimacy of the phone call. It is important to note that if you are being pressured to act immediately, hang up the phone, as it is most likely a fraudulent service.

In order to avoid phishing follow a few simple tips:

- **Spot the phishing attempt**: There are a few tell-tale signs of a phishing attempt. The first is that most of the offers are too good to be true. If the communication received involves lucrative offers or attention-grabbing statements, be careful. The second is a sign of urgency. If the communication tells you to act as fast as possible or that you have a limited time to do something, be cautious. Most reliable organizations give ample time before they terminate an account and they never ask patrons to update personal details over the Internet. When in doubt, visit the source directly rather than clicking a link in an email.

The third sign is a hyperlink or an attachment in the description. These links are not what they appear to be. If you are unsure whether a link is legitimate or not, do not click on it; do your own manual search of the link. Lastly, be wary of who you received the email, phone call, or text message from. As mentioned above, a lot of phishers pose as reputable and familiar companies or organizations. If anything seems out of the ordinary or suspicious, do not click on the email and/or hang up the phone.

- **Utilize browser settings**: the browser settings on your computer can be changed to prevent fraudulent websites from opening. This will allow only secure websites to be opened.
- **Add yourself to the do not call registry**: Place yourself on the do not call registry, and hang up or do not answer solicitation phone calls.
- **Do not give out personal information over the phone**: Phishers will not be able to take your information over the phone if you do not give it to them. If you think the phone call may be legitimate, ask them to provide information on the matter in writing.
- **Be skeptical**: If someone calls or emails you and requests very personal and valuable information for something you are unsure about, be skeptical about giving out your information. If the call or email is supposedly coming from a friend, family member, or an organization that you have a relationship with, call that person or organization and verify the validity of the request.

Please be aware of these potential threats. Should you believe you were contacted by a phisher, do not hesitate to call and report your suspicions to the Federal Trade Commission at (877) 382-4357 or FTC.gov/complaint. Also, forward all phishing attempts to spam@uce.gov and to the organization/person impersonated in the phishing attempt so they can notify others of the attempt.