

SCAM REFERENCE GUIDE



FRANKLIN LAKES POLICE DEPARTMENT
490 DEKORTE DRIVE
FRANKLIN LAKES, N.J. 07417
Main #: 201-891-3131
FAX: 201-891-0967

Detective Grassi
Office: 201-891-0048, ext. 2020
rgrassi@franklinlakes.org

DSgt. Jeffrey Jost
Office: 201-891-2701
jjost@franklinlakes.org

Computer Security Phone Scam

Scammers call your house and ask for you by name posing as computer security pros from legitimate companies like Microsoft or Windows Systems. They often use publicly available phone directories so they might know your name and other personal information when they call you. They might even guess what operating system you're using. The fake security experts claim that you're at risk for a computer security threat and offer to help you solve the problem. The criminals then ask you to perform a variety of tasks to help combat the bogus threat such as giving them remote access to your computer, tricking you into downloading malware, and even asking for your credit card information.

If you receive a call from someone claiming to want to help you fix your computer, you should take the following advice:

- Be wary of **unsolicited calls** related to a security problem, even if they claim to represent a respected company. Companies like Microsoft will **never** call you to correct a computer problem unless you have called them first.
- Never provide personal information, such as credit card or bank details, to an **unsolicited caller**.
- Do not go to a website, type anything into a computer, install software or follow any other instruction from someone who **calls out of the blue**.
- Ensure you have the latest security updates and Virus protection for your computer.
- Always use a strong, unique password and change it regularly
- Take the caller's information down and **report it to the Police**.

If you are suspicious or unsure do not hesitate to contact the Police Department for advice.

E-Mail Scams

These scams include fake email messages or websites that use the name of reputable companies or financial institutions. These email messages might look official and claim that you have won a contest, state that there is a problem with your bank account or credit card account or that you have inherited a large amount of money from an unknown relative. They will either request that you click on a link within the e-mail or call a phone number so that they can confirm your identity. The criminal will then instruct you to provide your personal information such as social security number, bank or credit card account number and logon information or password.

Do Not respond to these e-mails by clicking on a link, calling or replying to the sender. If you are concerned about your accounts contact your bank or credit card company using a phone number that you are familiar with or from an old statement or the rear of your credit card.

If you suspect that you've responded to a phishing scam with personal or financial information, take these steps to minimize any damage and protect your identity.

- Change the passwords or PINs on all your online accounts that you think might be compromised.
- Check with your Bank or Credit Card Company by using a phone number from an old statement or the back of your credit card.
- Place a fraud alert on your credit reports with Experian, Equifax and TransUnion.
- Do not follow the link in the fraudulent email message. A Financial Institution such as a Bank or Credit Card Company will never contact you through an e-mail regarding a security problem and they will never instruct you to click on a link in the e-mail to correct a problem.
- If you know of any accounts that were accessed or opened fraudulently, close those accounts.
- Routinely review your bank and credit card statements monthly for unexplained charges.
- If you receive a suspicious e-mail report it to your local Police Department.

Phone Phishing Scams

Common scenarios include:

- A grandparent receives a phone call (or sometimes an e-mail) from someone claiming to be a grandchild. If it is a phone call, it's often late at night or early in the morning when most people aren't thinking that clearly. Usually, the person claims to be traveling in a foreign country and has gotten into a bad situation, like being arrested for drugs, getting in a car accident or being mugged and needs money wired as soon as possible.
- Sometimes, instead of the "grandchild" making the phone call, the criminal pretends to be an arresting police officer, a lawyer, a doctor at a hospital, or some other person claiming to be involved in an accident and holding the person hostage until they get money for the repairs.
- Military families have also been victimized. After perusing a soldier's social networking site, a con artist will contact the soldier's grandparents, claiming that they had a problem while stationed away and they need money wired to them.
- While it's commonly called the grandparent scam, criminals may also claim to be a family friend, a niece or nephew, or another family member.

What to do if you have been scammed.

- Resist the pressure to act quickly.
- Try to contact your grandchild or another family member to determine whether or not the call is legitimate.
- Ask callers questions that only your real family members would know how to answer.
- Encourage your family not to post upcoming travel plans online, social networks.
- **Never** wire-transfer money to someone who calls unexpectedly, even if the caller claims to be a grandchild or other family member. Wiring money is like giving cash, once you send it you can't get it back.
- Contact your local Police Department for advice and to file a Police report.

Resources:

Federal Bureau of Investigations, <http://www.fbi.gov/scams-safety/fraud>

Microsoft Corp, <http://www.microsoft.com/security/online-privacy/phishing-scams.aspx>

Federal Trade Commission, <http://www.consumer.ftc.gov/articles/0376-hacked-email>