Digital You

Scam and fraud awareness

Unsolicited callers demanding payment

What it is: In this scam you typically receive a call from someone claiming to be from a government agency, demanding that you make immediate payment to them to satisfy a legal obligation. Two of the more prominent scenarios are:

- Caller identifies him/herself as the Internal Revenue Service demanding payment of an outstanding balance, OR
- Caller identifies him/herself as local law enforcement demanding payment of a fine for failure to appear for jury duty

In this scam the caller is generally demanding payment information (credit card, debit card or wire transfer) immediately and threatening criminal prosecution for failure to comply. Callers are generally very assertive and threatening.

What you should do: Do not engage these callers – hang up immediately. If you suspect that such an obligation exists, contact the government agency at their published phone number(s) to verify.
For the IRS-related scam:

- Refer to the following link for more information:
  http://www.irs.gov/uac/Newsroom/IRS-Repeats-Warning-about-Phone-Scams
- Refer to the following link to report the scam to the Treasury Inspector General's Office;
  http://www.treasury.gov/tigta/contact_report_scam.shtml

PC Technical Support Scam

What it is: In this scam you typically receive a call from someone claiming to be a computer technician with a technical support company. In some cases they will falsely represent themselves as affiliated with your internet service provider. They may tell you they have detected viruses or malware on your computer or offer a free security scan on your computer. Once you provide them with remote access to your computer they either attach malware which can steal your sensitive data or "lock" your computer and demand payment to "unlock."

What you should do: Never provide remote access to your computer under these circumstances. In all cases never engage such services without first verifying that the company is in fact genuine. Refer to the "Social Engineering" section below as well as the following FTC link:
http://www.consumer.ftc.gov/articles/0346-tech-support-scams.

Fake Website Phishing Scam

What it is: The typical scenario is that you receive a phone call, text message, or email enticing you to visit a website that appears to have an affiliation with AT&T or another company. In the case of a fake AT&T website, the enticement is generally the promise of a substantial bill discount or a gift card. Once at the fraudulent AT&T website, you are prompted to log in with your MyATT account credentials. The fraudster then uses the customer information obtained from the fake site to log into your account and make changes to the account or place orders.

What you should do: If you get this call or text message you should ignore it. Most importantly you should never use your AT&T account information to log into any website other than the AT&T website listed on your statement. Customers can report this activity to AT&T at *abuse@att.net*. If you have already been a victim of phishing, you can find information about filing a complaint with the Internet Crime Complaint Center (IC3) at *www.IC3.gov.*

"One-Ring" Callback Scam

What it is: Fraudsters use call generators with automated spoofing capabilities to place calls to a large volume of US cell phone numbers. The calls typically ring once. The number displayed on the recipient's caller ID is a high-cost international number, usually located in the Caribbean. If you call the number back you're greeted with a message designed to keep you on the line, such as "Hello, you have reached the operator, please hold." The longer you stay on the line, the more revenue fraudsters generate.

You may not realize you're calling an international number and that you will be billed for making an international call. Businesses are also victims because customers often use their work telephone to make the return call. Area codes used in the spoofed numbers are usually from Anguilla, Antigua, Barbados, British Virgin Islands, the Commonwealth of Dominica, Grenada, Montserrat, and the Turks and Caicos Islands. These countries' numbers are part of the North American Numbering Plan and do not require 011 to be dialed as with other international calls.

What you should do: Do not answer calls from numbers you do not recognize or initiate a return call. You will not be charged for receiving the calls. Companies that do not conduct business with companies in the above-mentioned countries may want to consider blocking these area codes to avoid this type of charge. If you have been victimized by this scam, file a complaint at *www.ftc.gov and www.IC3.gov.*