January 2013 Scams

The Internet Crime Complaint Center (IC3) and other organizations recently issued warnings about current scams. Here are a few of the current scams going around. As always, stay aware and stay safe.

Payday-Loan Repayment Scam

This scam involves victims being relentlessly contacted at their residences and places of employment regarding claims that they are delinquent on a payday loan. The scammers use various coercion techniques to persuade the victim to send money, such as repeated phone calls, abusive language, and threats of bodily harm and arrest.

There are two troubling concerns with this scam. First, the scammers use information acquired from legitimate online loan applications to trick their victims into believing that they are being contacted by actual representatives of their loan providers. Second, the coercion tactics used by the scammers are becoming increasingly aggressive and frequent. They've even escalated into telephone denial-of-service (TDoS) attacks against the victims' employers, some of which are emergency service agencies. An FBI alert recently warned that the TDoS attacks have tied up the emergency services' telephone lines, preventing them from receiving and responding to legitimate emergency calls. The alert also says that such attacks have "created a threat to emergency services across the nation."

Tech Support Scam

Although the Federal Trade Commission shut down six tech-support scammers in October, victims are still receiving telephone calls from scammers claiming to be with Microsoft Tech Support. The callers have very strong accents and use common names such as "Adam" or "Bill." Callers report the victim's computer is sending error messages, and a virus has been detected. In order to gain access to the victim's computer, the caller claims that only their company can resolve the issue. The caller may convince the user to grant them the authority to run a program to scan their operating system. Victims watch the caller going through their files as the caller claims they are showing how the virus has infected their computer. Victims are told the virus could be removed for a fee and are asked for their credit card details. Those who provide the caller remote access to their computers, whether they paid for the virus to be removed or not, report difficulties with their computer afterwards due to malicious software.

Tax-Related Identity Theft

It's that time of year again—tax-related identity theft season. The number of known incidents has increased more than twelvefold since 2008, according to a recent study from the U.S. Government Accountability Office. More than $5.2 billion of taxpayer money went to fraudsters who filed fake returns in 2011, according to the Wall Street Journal. Tax ID thieves may use the victim's name and stolen Social Security number to collect a refund in the victim's name, create a fake IRS or accounting website to con

unsuspecting taxpayers into filing their returns online, or send a phishing email spoofing the IRS that asks for the victim's personal information.

Protect Yourself

Follow these safeguards to help protect your identity:

- Shred everything with your name and address, including statements and invoices, receipts, pre-approved credit offers, credit-card checks, and insurance-related materials. ISPO recommends using a quality ***crosscut*** shredder.
- Protect your personal information. Don't email Social Security or credit card numbers. Use anti-virus software to protect your PC from malicious software that could capture your keystrokes. Pick strong passwords, change them often, and don't use the same ones for different websites.
- Keep sensitive paper-based information, like bank or credit card statements, passports, Social Security cards, birth certificates, locked up. Always be aware of who has access, such as household employees, work crews, and even family members.
- Check your credit reports early and often. Visit annualcreditreport.com, the government-mandated source for free credit reports. Investigate suspicious activity and stay on top of it until the matter is resolved.