Latest Scam Roundup | Exposing Cyber Schemes

By Denise Richardson

Today's scams seem to be multiplying like rabbits. It seems like no matter how advanced law enforcement officials get at recognizing scams, fraudsters and thieves always find new ways to steal data or take hard-earned money from honest individuals and businesses. There are a few scams that have been in the news lately that you should be aware of. Share these risks with others, especially since they prove that anybody can be the target of these and other scams designed to steal your money, data and identity.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

The IRS has reported an increase in the occurrence of a Social Security and tax fraud scams.

The scam artist contacts primarily older individuals and others who receive Social Security benefits, pretending to be an income tax preparer and offering them a larger refund if they use the "services" that the scammer offers. All the victim has to do is pay the up-front filing and processing fees to have their taxes professionally prepared. The larger refund looks good on paper, but unfortunately that's the only place it looks good; the deductions and withholdings entered in the return to end up with that large refund are fake and will be rejected by the IRS. By the time the victim finds this out, however, the scammer is already gone with the up-front payments he received.

The Internet Crime Complaint Center's (IC3) September Scam Alert warns of a few recently reported crime trends and new twists to previously-existing cyber scams.

Mass Joinder Lawsuit Scams

This particularly disturbing scam takes advantage of homeowners, many of which are struggling to avoid foreclosure or fighting to overcome abusive mortgage servicing practices. Scammers love targeting anyone in a tough spot and though this scam is currently making the rounds in California -it will surely find its way throughout the states.

Potential victims receive letters informing them that they have an opportunity to take part in a class-action lawsuit against an unscrupulous mortgage lender. Promising big rewards upon the settlement of the lawsuit, the victim is asked to provide between $2000 and $5000 in up-front legal fees to secure their place in the lawsuit. Of course, those who join in with legitimate class-action lawsuits aren't asked to pay anything to join since the legal fees of any attorneys involved in the lawsuit are taken out of the settlement amount. For those who fall for this scam, the scam artist not only takes off with their money -but often their last hope in saving their home from a wrongful foreclosure.

Online auction websites are popular places for scams, and a new phishing scam has been making the rounds while pretending to be correspondence for popular sites. Potential victims receive emails that appear to be from the site, confirming the posting of their ad for a "Sony Playstation 3 Metal Gear Solid 4 PS3 80 GB Bundle." Those who respond to inform the sender that there's a mistake are at risk of being added to spam email lists or having their personal login information compromised if they provide any credentials for the site the email purports to be from. Those who click on imbedded links -open themselves and their computers to malicious malware that can open access to contacts, passwords, account numbers and more.
Fraud Trends Affecting The eCommerce Community

A surge in fraudulent transactions by scammers has also been plaguing other online retailers, so those who operate e-commerce sites should be on guard too. According to IC3.gov, these frauds have been occurring lately in one of two ways;

Email addresses leaked by the hacker groups Anonymous and LulSec in July of this year, are now being used to place fake orders, with the majority of the addresses being military email addresses which had in the past been considered less likely to be fraudulent than other address types.

The other way that scammers are trying to pull one over on e-commerce sites is through the use of "tagged" email addresses; these "tags" are address add-ons that can be added to allow multiple variants of a single email address to be used without the need for creating a new account. This allows multiple transactions to be made quickly without the work of setting up a new account each time, letting the scam artist try and scam a site multiple times from the same email address. Both of these scams allow the scammer to use fake or stolen payment and processing information to place orders, so if you notice a large number of military orders or orders with nearly identical email addresses then you should be suspicious.
According to law enforcement officials;

The purpose of e-mail tagging is to allow consumers to have one e-mail address for every purpose. The attractive feature of e-mail tagging is it allows the consumer to vary their e-mail address to help differentiate when placing orders, shopping, working, schooling, etc., but automatically forwards to the primary e-mail address. This feature on Gmail works in two ways, either with a period or a plus sign. The period works by allowing the consumer to take an e-mail address, JohnDoe@gmail.com, and add as many periods as the consumer wants to the e-mail address, JohnDoe.....@gmail.com, J.o.h.n.D.o.e@gmail.com, etc.

Visit IC3.gov for additional info on email tagging and email tumbling.

In light of the various weather related disasters, the Internet Crime Complaint Center further reminds the public to beware of fraudulent emails and websites purporting to conduct charitable relief efforts. For more info see: Tips on Avoiding Fraudulent Charitable Contribution Schemes.

To learn more about internet safety and how to avoid cyber related fraud and find resources for businesses and individuals of all ages, visit the National Cyber Security Alliance at StaySafeOnline.org.

For more scam alerts, trends and descriptions see: Scams & Hoaxes & Known Scams and Avoid Fraud.

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.