

Protect Yourself From Online Scam Artists

By Scott Derksen, VP Technology, IRON Solutions, LLC

E-mail and Internet are great resources that have revolutionized the way humans communicate, market products, and access information. Unfortunately, it has also proven to be a very fertile medium for the unscrupulous and the morally challenged.

Scammers regularly use e-mail and online response forms from your website or online advertising in attempts to steal money or personal information from unsuspecting victims. Both the experienced and those less experienced in the ways of the Internet have fallen prey.

Recently, we have seen an increase of this type of activity targeting equipment dealers, so I thought I would collect some information to help us all to recognize scam attempts and online fraud. What follows is a combination of some reading I did today and some recent experiences we have helped our customers deal with. The good news is that it is not difficult to learn how to recognize these scam attempts.

Here are descriptions of four of the most common types of online scams as well as some general indicators that should help you recognize trouble when it approaches you.

Bogus Purchase Scams

In the bogus purchase scam, you receive an e-mail or an online response form from a prospect who has visited your website or saw your product available for sale online. The most common ways this goes wrong are the overpayment scam and the falsified payment instrument.

For any transaction you are considering, keep these tips in mind:

- 1) Never accept a cashier's check without verifying by telephone from the issuing bank that the check is bona fide. There are several schemes in existence using falsified cashier's checks.
- 2) Don't accept any payment method that requires you to "give back" an amount representing an "overpayment" made for your equipment. This includes freight overpayment portrayed to make your life easier.
- 3) The only reliable methods of receiving payments from overseas or domestic buyers is a wire transfer into your account before the goods are shipped out or a bank letter of credit from the buyer's bank to your bank. Have your bank review it for any clauses that would be difficult to comply with. In domestic sales you may take other instruments, but make it a condition of the sale that you hold the item until your bank confirms that the cash has been secured.
- 4) For an overseas sale, make sure you get the telephone number, name, and address of the U.S. forwarding agent to be used by the buyer.

The number one rule to remember when making an online sale is that if something seems fishy or too good to be true ... you're probably right. Don't assume that phone contact validates an identity either – many recent scam reports have ongoing phone conversations over months. Ask for some North American supplier references. A good buyer will not be offended by your doing some homework.

Phisher Scams

In the phisher scam the main target is your information, which will be used to do you financial harm. You receive an e-mail from a bank/online service provider/financial institution that asks you to click a link and

visit a website in order to provide personal information. Such an e-mail is more than likely the type of Internet scam known as "phishing." A phisher scam is one in which victims are tricked into providing personal information such as account numbers and passwords to what they believe to be a legitimate company or organization.

In order to carry out this trick, the scammers often create a "look-a-like" website that is designed to resemble the legitimate company's official website. Be wary of any e-mail that asks you to click on a link and provide sensitive personal information such as banking details.

Information submitted on these bogus websites is harvested and may then be used to steal funds from the user's accounts and/or steal the victim's identity. Most legitimate companies would not request sensitive information from customers via e-mail. Do not click on the links in these e-mails. Do not provide any information about yourself. If you have any doubts at all about the veracity of an e-mail, contact the company directly.

Nigerian Scams

With the Nigerian or "419" scam, you receive an e-mail/letter/fax that asks for your help to access a large sum of money in a foreign bank account. The message says that you will get a percentage of the funds in exchange for your help. The "large sum of money" does not exist. The messages are an opening temptation designed to draw potential victims deeper into the scam. Those who initiate a dialogue by replying to the scam messages will eventually be asked for advance fees supposedly required to allow the deal to continue. They may also become the victims of identity theft. The scammers use a variety of stories to explain why they need your help to access the funds ranging from political climate to a charitable angle to suggesting you are a distant relative entitled to the money.

If you receive one of these scam e-mails, it is important that you do not respond to it in any way. The fraud perpetrators are likely to act upon any response from those they see as potential victims and it is likely to waste a lot of your time, or worse yet, set you up as a target.

Lottery Scams

In the lottery scam, you may receive an e-mail/letter/fax that claims you have won a great deal of money in an International lottery, even though you never bought a ticket. The e-mail may claim that your e-mail address was randomly chosen out of a large pool of addresses as a "winning entry." Such e-mails are almost certainly fraudulent. In some cases, the e-mails claim to be endorsed by well-known companies such as Microsoft or include links to legitimate lottery organization websites. Any relationships implied by these endorsements and links will be completely bogus. There is no lottery and no prize. Those who initiate a dialogue with the scammers by replying to the messages will first be asked to provide a great deal of personal information.

Eventually, they will be asked to send money to cover expenses associated with delivery of the supposed "winnings." They may also become the victims of identity theft. DO NOT respond to these messages. DO NOT supply any personal information to the scammers.

General Scam Indicators

The scams described above are some of the most common types of Internet fraud. However, these are very clever people who may use many variations of these concepts to achieve their less than admirable goal of parting you and your money.

In general, be wary of any offering that promises you money, jobs or prizes; asks for donations; proposes lucrative business deals; asks you to provide sensitive personal information; or asks you to follow a link to a website and log on to an account.

In closing, trust your instincts. If something sounds too good to be true, more often than not it turns out to be the case. If an equipment dealer comes across any specific cases of these sorts of activity, I encourage them to visit the secure area of www.irondealer.com to discuss it in our spam alert discussion area. There you will find details of current scam artists and you may help another dealer avoid a problem.

Editor's Note: This article was reprinted with permission from the *IRON Solutions Customer Newsletter*, March 2006. IRON Solutions may be reached at 636-343-8000 or toll free at 877-266-4766.