Common Scams Targeting Small Business Owners
by Esco Buff, PhD, APF, CF

Scammers will often go to great lengths to convince anyone that their offers or requests are legitimate. Many scammers might even try to trick you by appearing to have personal information about you such as your date of birth, social security number, mother's maiden name, etc. Therefore, it's important that you remain aware of typical scams and know what to do if you or your farrier business is targeted.

Tax Refund Scam
In this scam, the scammer will typically pretend to be from a government agency, bank or private law firm claiming that you are entitled to reclaim your overpaid tax or bank fees. The scammer may even tell you that your refund is taxable and you will have to pay the tax amount before receiving the tax refund or that you have to pay a fee to receive your money.

Credit Card and Overpayment Scam
This scam involves the scammer contacting you to purchase goods and services. The scammer then sends you a payment by check, money order or credit card for more than the agreed price. The scammer then asks you to refund the overpayment. The scammer is hoping you will transfer the refund or pay them before you discover that the check has bounced or that the money order or credit card was a fake. If you sell supplies, you have to be on the look-out for unusual or complicated orders from overseas.

Unauthorized Advertising Scam
This scam involves the scammer sending you an invoice by mail, fax or email for a listing or advertisement in a magazine, journal or business register which you didn't authorize or request. Scammers will send a proposal for a subscription, disguised as an invoice or renewal notice for an entry on a website or trade directory. Often the business is based overseas. It may sound like a free entry, but charges can be hidden in the fine print, resulting in demands for payment later.

Office Supply Scam
This scam involves you receiving and being charged for goods that you did not order. These scams often involve goods or services that you regularly order such as paper, printing or office supplies. You might receive a phone call from the scammer claiming to be your regular supplier, telling you that this offer is a special or is available for a limited time only. If you end up

agreeing to purchase any of the supplies that are offered, you will often find out they are overpriced and of poor quality.

Website Domain Name Scam

In this scam you'll be sent either an unsolicited invoice or email for an internet domain name registration usually very similar to your own business domain name, or you'll be sent a renewal notice for your actual domain name. The notice could be from a business that supplies domain names trying to trick you into signing up to their service or it could be from a scammer trying to take your money.

Online Transaction Scams

Online scams can include auction and shopping scams, spam offers such as junk mail or free internet offers, online banking scams using spyware or key-loggers; and credit card order scams from overseas. Many of these scams occur without business owners being aware of them until it's too late. Always be wary of any offers over the internet promising anything for free or asking for your bank details.

Charity Scams

Charity scams often occur around times of emergency, such as after major disasters like floods, fires or other weather related disasters. Scammers pose as not-for-profit organizations collecting money for victims of these and other disasters. Genuine charities are registered in their state and are able to give you full contact details, tax status, as well as a receipt for your donation.

How to Protect Yourself

Being aware of the above scams is your first line of defense as well as reviewing the latest scams posted by The Council of Better Business Bureau (BBB) and the US Government (USA.Gov). Some other common ways to protect yourself and your farrier business are as follows:

- Be suspicious of any unexpected, complicated or suspicious orders from overseas.
- Be wary of payments which involve a number of credit cards.
- Only accept the invoiced price and do not send the goods until the payment has been verified by your bank. Your bank can provide assistance on how to verify that the credit card number is valid.
- Only deal with trusted freight companies (like USPS, UPS, FedEx) that you can contact to obtain details.
- Do not send money or money transfers to anyone you do not know or trust.
- Do not respond to unsolicited e-mail.
- Do not click on links contained within an unsolicited e-mail.

- Be cautious of e-mail claiming to contain pictures in attached files as the files may contain viruses.
- Contact the actual business that supposedly sent the e-mail to verify that the e-mail is genuine.

How to Report a Scam

In the event you become aware of or a victim of a scam, the first thing to do is report it. By reporting the scam to the appropriate governmental agency, you can help them identify scammers and warn other businesses.

To report potential e-scams (scams over the internet) contact: The Internet Crime Complaint Center at http://www.ic3.gov/complaint/default.aspx.

For a list of all sorts of frauds, how and who to contact, go to: The Financial Fraud Enforcement Task Force at http://www.stopfraud.gov/report.html or call (202)-514-2000.

Scammers continue to use a wide variety of tactics to try and separate you from your money. There are several resources available to help you check out a company before you become a victim or to help you file a complaint if you have a problem. A good place to start is with the references listed below. The web sites of these agencies often have databases that allow you to look up complaints against all kinds of businesses. You can also file a complaint to warn others or if you have become a victim of a scam. In some cases, you may even get help at getting some of your money back.

References

Council of Better Business Bureaus (BBB) for BBB Scam Alerts -
http://www.bbb.org/council/news-events/bbb-scam-alerts/2014/01/target-data-breach/

USA.Gov for Scam Alert: Targeting Small Business -
http://www.usa.gov/topics/consumer/scams-fraud/business/small-business-scams.shtml

FBI for New E-Scams and Warnings –
http://www.fbi.gov/scams-safety/e-scams