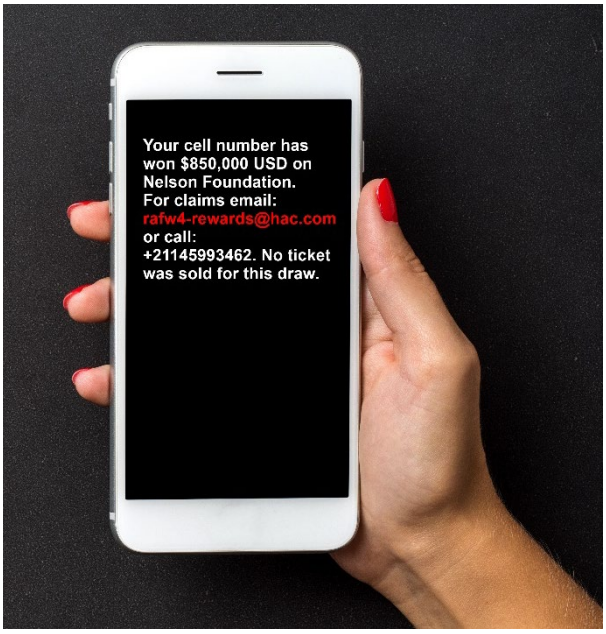
CyberAlert

January 6, 2020

Beware of the Latest Phone Scams

Risk Management Question: Fraudsters seeking to take your money or personal information use a variety of phone scams, including SMSishing (text-based phishing). How can you and your employees protect against phone scams?

The Issue: Phone scams manifest in a variety of ways, but one constant is scammers trying to get money or personal information from you. SMSishing has become a very popular tool for scammers, but it is only one of a number of strategies available to them.



Often, fraudsters pretend to be a member of law enforcement or a federal agency such as the IRS. They claim that you will face harsh consequences for not paying taxes or some other form of debt, and they may ask you to provide personal information. Their goal is to scare you into complying with their demands.

Another scam involves claiming that the target individual has been selected to receive a special offer. The offer will seem like a great deal, but the target will be told that it is only available with immediate payment. These scams rely on the time-sensitive nature of the "deal" in order to coerce victims into falling for the scam.

Others scammers may claim that you have won a prize, but in order to collect it, you have to pay a small administrative fee, or pay for the "shipping" to receive your prize. Of course, after the money has been transferred, the scammer will not respond to any further contact.

Risk Management Solutions:

Here are some things to keep in mind if you receive a suspicious phone call or text message:

- The IRS will never contact you by phone. It sends send all notifications and alerts via USPS letter.
- Never provide any personal information over the phone, even if the caller claims to be a member of a federal agency.

HINSHAW

- If the caller asks you to wire money, or to use any other form of payment that is difficult to trace (prepaid card, money transfer app, gift card, etc.), hang up.
- Most legitimate businesses will give you time to think about their offer before asking you to commit. Do not get pressured into making a decision on the spot.
- Never click on links sent via text message, especially from people you do not know.

One relatively easy security measure is to register your phone on the National Do Not Call Registry. While this will not stop all spam calls, it should reduce them. More information and registration information can be found at https://www.donotcall.gov/.

Happy New Year from Hinshaw! And remember, always think before you click.

Steven M. Puiszis
312-704-3244
spuiszis@hinshawlaw.com

Noah D. Fiedler
414-225-4805
nfiedler@hinshawlaw.com

Annmarie D'Amour
212-471-6231
adamour@hinshawlaw.com