AIM

AIM CYBER
High-touch services to help you navigate modern cyber threats.

SMISHING - THE NEW PHISHING

Most of us are familiar with phishing, emails that appear to come from a company executive, government agency or other official saying we need to send private information immediately to rectify a problem. Or they offer information we all want by clicking a link.

Of course, the real purpose is to steal your personal information or your credentials, or to download malware, or all of them.

Smishing is a variant of phishing that uses text and SMS messages instead of emails. The intent is the same, only the delivery method differs. For simplicity, when I refer to text messages, SMS messages are included.

Phishing is popular because it works. Enough people fall for it to make money for the scammers. In some cases, significant amounts of money.

However, more people are getting wise to phishing and check if an email comes from who it says it does. An easy way is to click on the arrow in the sender field. If the displayed email address doesn't match what appears in the Sender field, it is probably a scam.

So why smishing? You don't need to know someone to send a text message. Cybercriminals can send text messages to random phone numbers and the message will be received.

If you know the sender what will show is their name. Otherwise, it is just a phone number that shows.

And a phone number gives little help in identifying the sender. Short code services reduce the phone number to 6 or 7 digits making it virtually impossible to know who sent it.

The other issue with smishing is if they include a link to click, it is often shortened using a service like bitly or Google's shortening service which assigns a shorter link address. Shortening services are often used for legitimate purposes but in this case, the intent is to disguise the real url, (web address). For instance, if the text message claims to be from your bank but the link is https://www.badsite.com, it is doubtful you would click it. But if it was https://goo.gl/abcdefg you would not know where you were being sent and may be more tempted to click.

The best way to prevent people from falling victim to a smishing attack is through training and then sending test smishing messages and see who clicks.

Want to learn more about cyber security and education, contact AIM Cyber at info@AIMglb.com or call (888) 773-1920.