Please Read!

Scam Of The Week:

Phishing Moves To Smishing

Brunswick State Bank
Brunswick\Winnetoon

Internet bad guys are increasingly trying to circumvent your spam filters and instead are targeting your users directly through their smartphone with Smishing attacks, which are hard to stop.

The practice has been around for a few years, but current new scams are mystery shopping invitations that start with a text, social engineering the victim to send an email to the scammers, and then get roped into a shopping fraud.

These types of smishing attacks are also more and more used for Identity theft, bank account take-overs, or pressure employees into giving out personal or company confidential information. Fortune magazine has a new article about this, and they lead with a video made by USA Today which is great to send to your users as a reminder.

"Bad guys are increasingly targeting you through your smartphone. They send texts that trick you into doing something against your own best interest. At the moment, there is a mystery shopping scam going on, starting out with a text invitation, asking you to send an email for more info which then gets you roped into the scam.

Always, when you get a text, remember to "Think Before You Tap", because more and more, texts are used for identity theft, bank account take-overs and to pressure you into giving out personal or company confidential information. Here is a short video made by USA Today that shows how this works: https://www.youtube.com/watch?v=ffck9C4vqEM
Obviously, an end-user who was trained to spot social engineering red flags (PDF) would think twice before falling for these scams. The link goes to a complimentary job aid that you can print out and pin to your wall. Feel free to distribute this PDF to as many people as you can. Let's stay safe out there!