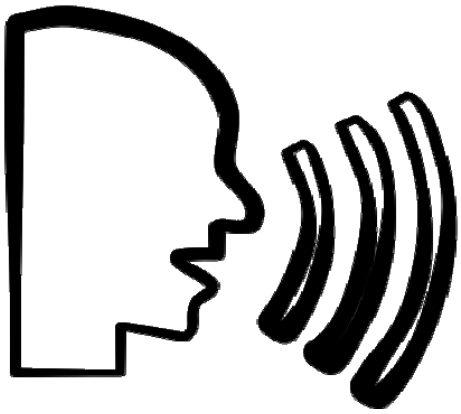
In this issue:

First Bank & Trust Company
The Bank That Puts You First
Member FDIC

February 2017 Volume 3, Issue 2

Say What?

A New Software That Can Change What You Say



Late last year, Adobe revealed a new software tool that may change how we deal with social engineering, called Project VoCo. VoCo is essentially Photoshop for voiceovers and it's a very interesting concept. Let's say you create a video, but after viewing and listening to it, you want to change what you said. For example, maybe you watch your old wedding video or a taped speech you gave and you forgot to thank someone or left out a couple of important points. You can't change what you said since it's already been recorded…or can you? Thanks to Adobe's new VoCo software, you can now edit video or add verbiage via text!

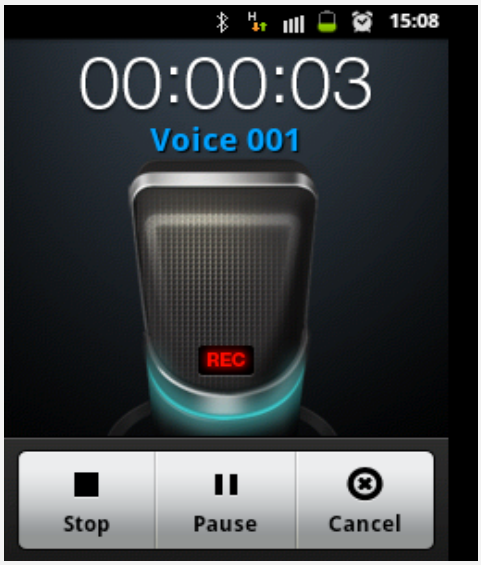
It is an absolutely fascinating advancement in technology and a total dream for TV producers, sound engineers and video editors. Adobe has been the mastermind behind photo editing, allowing for the creation of abstract pictures and visuals that look like reality, manipulating backdrops and even adding or removing objects in pictures. Adobe has made the tool so easy to use that not only can graphic designers have fun, but kids of all ages are able to change their photos to look like whatever they want! Now, Adobe has applied that thinking to the audio aspect of editing technology.

VoCo has the capability via algorithm to understand the makeup of the voice that has been recorded and replicate it to add words that were not spoken in the original recording as long as the recording is at least 20 minutes long. However, while many are extremely excited about this new technology, there are equal amounts of people who are not thrilled and see this as an open door for a new wave of social engineering attacks. Cyber criminals are always looking for new methods to penetrate through networks and some see this software as one more tool they can add to their arsenal.

Experts believe that one example of how VoCo can be used as an attack is through voicemail. For example, if a CEO left a voicemail for someone in the accounting department, and a hacker found their way into the system, they could change the voicemail to say something that may end up hurting the institution, such as giving instructions to transfer funds to a particular account. The information received would most likely not even be questioned because the directive is coming from who they believe to be the CEO.

Continued on page 2

Another example would be the interference with voice activated devices. IoT (internet of things) has become more popular and has led to the creation of Amazon Echo and Google Home. Many companies are embracing IoT as well and are implementing the technology in their own products such as Microsoft Xbox OneS, smart TVs and smart cars. A hacker could possibly get through a company's network connection and provide voiceover instructions that could result in a loss of data, trade secrets and confidential information.



It is important to note, Adobe is still in the beginning phases of this technology and are addressing some of the security concerns by trying to make it easy to detect if the voiceover has been maliciously interfered with by using watermark technology. While they work through the kinks and try to make it as secure as possible, it is important to remind employees that technology is ever-changing and to stay vigilant against social engineering attacks such as phishing and vishing which are extremely common. VoCo could be the new type of social engineering that everyone has to worry about in the near future, but educating and training employees will help them distinguish between what is legitimate and what could be a potential threat.

Sources:
http://www.bbc.com/news/technology-37899902
http://www.zdnet.com/article/adobes-voco-voice-project-now-you-really-can-put-words-in-someone-elses-mouth/

7 Best Social Media Practices

Twitter, Facebook and LinkedIn are part of our new normal. These social media platforms help us connect with friends and family, find jobs and share experiences. Social networks have become a powerful tool for everyone., but security is also an issue with these forms of communication. Hackers have found a way to exploit these methods of communicating, making it sometimes risky for people to share some of the best moments of their lives. Although social media provides great benefits, like with most things, there are also safety concerns. Below is a list of 7 best social media practices that will help keep you safe while staying connected to friends and family.

1. Be careful of links you receive via direct message. Social media sites are a hotbed for phishing attacks. Although the link may seem legitimate, treat it the same way you would a treat a link you receive by email. If it looks suspicious, just delete it.

2. Don't divulge too much information. Yes, it is fun to post photos of recent trips or funny snip videos of your dog doing something crazy, but sometimes that is exactly the information a hacker needs to break into your accounts. Hackers usually go the route of "forgot your password" to try and steal information. The information you provide on social media may give them some hints on what your password could be just by scrolling through your timeline. As a precaution, you should never share what city and state you were born, home address, social security number, date of birth or any financial information.

3. Be selective of who you "friend" on a social media sites. There are tons of fake profiles created by cyber-criminals just so they can troll around and look for their next victim. This is an easy way to steal someone's identity.

4. Whatever you post will most likely be there forever. Think twice before posting something. Just because you delete it does not mean it's gone. The internet is very fast moving and whatever is posted can easily be printed and images and videos can be saved to computers for everyone to see, including future employers.

5. Do not allow social media networking services to scan your e-mail address book. Normally when you join a social media site they ask to scan your inbox so you can invite your contacts to "follow" or "friend" you. If you agree everyone in your contact folder will receive an email from that site.

6. Check your privacy settings. Many of the sites allow you to customize your settings to limit who and what groups can see various aspects of your personal information.

7. Educate, Educate, Educate. Kids love social media! Playing games and anything that looks intriguing to their eyes can potentially be very dangerous. Talk to your kids about avoiding clicking on links that promise great "prizes" or playing games that may post or share information without your knowledge. If it seems too good to be true, then it probably is. Many of these games and contest are a direct link to a phishing scams.

Sources:
http://seniornet.org/blog/11-tips-for-social-networking-safety/
http://www.networkworld.com/article/2346606/microsoft-subnet/12-tips-for-safe-social-networking.html