the majestic
of Downtown Baldwin Park

NEWSLETTER - AUGUST 2017

NEW SOCIAL MEDIA SCAMS: CAN YOU TELL FRIEND FROM FOE?

Scams on social networks are nothing new, but they're constantly changing to take advantage of the latest apps, trends and news. As with all social engineering scams, the best defense is a skeptical user.

Most security organizations have long since lost the fight to keep employees from using social media on work computers; indeed, many people now have to be on Facebook or Twitter as part of their professional duties. The goal now is to help contain any damage from social media attacks—keeping in mind that even an attack via someone's personal account can affect their work lives.

To that end, we spoke to some security pros about scams and attack vectors that are springing up on social media. Here are their tips for avoiding social media scams.

Social media accounts aren't a shortcut to riches. The world of con artistry has seen endless variations of the get rich quick scheme. SEO expert Bradley Shaw points to one current example on Twitter, the "Twitter cash starter kit," which promises users that they can hit it rich on the platform in unspecified ways. The key to the scam? "Victims will pay an initial fee for the kit itself by entering their debit or credit card information," says Shaw. Once the scammer has access to that information, charges quickly mount: "Their cards are charged a hidden 'membership' fee of $50 each month after initial signup. They can also make further fraudulent charges."

You can't win a contest you never entered. There are plenty of "free" too-good-to-be true enticements that can woo the unwary as well. J.A. Hitchcock, president of WHOA and WHOA-KTD, a volunteer organization that fights online harassment, notes one scam becoming increasingly popular on Snapchat. "A user gets a graphic that claims they are a winner. When they click on the graphic and fill out requested info, they're asked to download an app in order to receive a prize. That app most likely contains a virus."

Reminders

* First day back to School for Orange County Monday August 14th.
* Save some time, pay your rent online! Every resident is furnished with an online Resident Portal account so you can not only online pay your rent online, but enter in maintenance requests as well. If you don't have one or need help accessing yours, please email majestic@leclairinc.net
* It's hot out and we are using our AC's more. Please remember to change you AC filter monthly.
* Save this in your phone! Afterhours maintenance line (for emergencies only) – **407.274.6650**

Beware of wolves in brands' clothing… One particularly devious scam involves imitating a business's social media presence. "Fraudsters step up and grab unclaimed businesses on social media and act as the owner," says Julian Wong, architect at fraud detection provider DataVisor. "Someone looking to book an appointment at a spa reaches the fraudster instead of the legitimate business owner, who then takes the caller's credit card info as a 'down payment' to book or hold the appointment and then runs off with the money."

...especially if they're offering help. One scam exploits an aspect of life we've come to expect and rely on—that sometimes brand accounts seek you out, not the other way around. Companies ranging from cable providers to airlines automatically search social media to find people complaining about their services and then use support accounts to reach out and try to resolve issues. But those complaint tweets are public and those search tools are available to anybody. Philip Tully, senior data scientist at ZeroFOX, a company that detects risk on social media, outlines how this can get scary: a fake "support" account, with graphics and a bio borrowed from a real one, reaches out to someone having problems, asking them to log into a phishing site where they give their account number and password.

You reveal more about yourself than you think. A variation on this scam involves trying to assess a user's public profile to determine potential commercial interests. "A hacker can scan a Twitter feed to find out that a user posts constantly about her new puppy," explains Keeper Security CEO Darren Guccione. "The hacker then creates a phishing scam that looks like a product announcement for a portable puppy crate and targets that Twitter account."

Social platforms can't keep up. Even things that seem to have a platform's seal of approval—like a paid advertisement—hasn't necessarily been vetted; the ad-buying process is wholly automated and usually pretty cheap, and offers a great chance to get phishing links in front of targeted user demographics. "Up-front cost to the perpetrator pales in comparison to their ROI," says Tully. "On Twitter, advertisers pay only when a user engages with a promoted Tweet, and the average cost of each engagement ranges between $0.50 and $2.

Perpetrators in successful phishing campaigns make off in some cases with thousands to tens of thousands of dollars in profit from things like credit card fraud or direct money withdrawal, so it only takes a single victim to make a spray and pray attack worth it."

Think twice even when you see someone you know. Lindsay Satmary, a blogger at Paperclips and Pacis, warns about profile cloning—scammers creating a duplicate profile for a real person in the hopes of getting that person's acquaintances to accept friend requests, giving them a trusted position in their social networks. Kevin Lee, trust and safety architect at fraud prevention software provider Sift Science, says that some attackers go one step further, compromising real accounts to spread malware and spam.

Expect social espionage. Once attackers have infiltrated a circle of friends or professional associates, they're in a perfect position to monitor networks. "Hackers can use social media to infect someone within an organization, then sit on the network and monitor their internal communications," says Asaf Cidon, VP of content security services at Barracuda Networks. "This can be carried out by impersonating a real individual,

adding them as a friend on LinkedIn, or even joining an open forum or channel on a social platform like Slack."

The endgame is often a phishing attack. "Hackers can go on LinkedIn and create fake accounts posing as a current or former employee at your company," says Kurt Wescoe, chief architect at Wombat Security Technologies. "The hacker then attempts to contact multiple people at your business, collecting small amounts of data from each employee. Each bit of info on your company—location, office hours, hierarchy, email nomenclature—could potentially add up to enough info for a successful attack." Cidon describes a specific scenario: "If hackers know the exact timing of a deal that is underway and who's in charge of authorizing the wire transfer, they're able to initiate a spear-phishing attack at the most opportune time."

"With the adversary constantly evolving, together with the massive volume of new content pouring across their platforms, social networks only have so much control over these types of problems," says ZEROFox's Tully.

The bottom line in all these scams: Keep your guard up. Social media sites are designed to be as friendly as possible, but you lose many of the cues that help you tell friend from foe in real life. Being aware of these techniques can help you and your co-workers stay suspicious enough to avoid them.

 By Josh Fruhlinger

CSO | Jun 23, 2017 3:41 AM PT

Original article https://goo.gl/rZ4jEu

Community Reminders

- Save this in your phone! Afterhours maintenance line (for emergencies only) – 407.274.6650
- Reporting of Maintenance concerns: To ensure all maintenance requests are received, and addressed as quickly as possible call the office to report any issues that need to be addressed. If you have online portal access you can also log your work order on line. Please do not stop the maintenance staff while on another task, as it may not get entered into the system correctly or in a timely manner, causing a delay in their current work order and delaying the response of your request.
- Reminder to all Pet Owners, you must keep your dog on a leash at all times when on the property and you must clean up after your pet. There are pet stations located on the property for your convenience. If anyone knows who is not cleaning up after their pet please contact the office so we can address it directly with that resident.

REESE'S™ PEANUT BUTTER CUP ICEBOX PIE

Ingredients

Crust

1 cup finely crushed mini pretzels (about 3 cups)

1/4 cup packed brown sugar

1/2 cup butter, melted

Filling

1 box (6-serving size) chocolate instant pudding and pie filling mix

2 cups cold milk Save $

3/4 cup creamy peanut butter

Topping

1 1/2 cups (from 8-oz container) Cool Whip™ frozen whipped topping, thawed

1 tablespoon creamy peanut butter

1 tablespoon chocolate-flavor syrup Save $

3/4 cup (from 8-oz bag) Reese's™ peanut butter cups miniatures, unwrapped

Steps

1. Spray 9-inch glass pie plate with cooking spray. In medium bowl, mix Crust ingredients. Press mixture against bottom and side of pie plate. Refrigerate 10 minutes.

2. In large bowl, beat pudding mix and milk with whisk 2 minutes. Beat in 1/4 cup of the peanut butter. Let stand 5 minutes.

3. In small microwavable bowl, microwave 1/2 cup peanut butter uncovered on High in 15-second increments until thin enough to spread. Spread warmed peanut butter over chilled crust. Pour chocolate pudding mixture into chilled crust; spread evenly. Cover and refrigerate 3 hours.

4. Just before serving, spread whipped topping on top of pie. In small microwavable bowl, microwave 1 tablespoon peanut butter uncovered on High in 15-second increments until thin enough to drizzle. Drizzle warmed peanut butter and chocolate syrup on top of whipped topping. Top with peanut butter cups. Cover and refrigerate any remaining pie.