Social Media Exploitation Low Tech

Hello readers,

Security is an issue on many levels of the internet. Emailed links can be a source of spearfishing data, insecure connections can allow people access to your networks. Today we're talking about a different kind of internet deception. Social Media and it's more deceptive practices. To begin to evaluate what risks it poses to you personally or professionally you'll need a brief overview of the kind of exploits and social engineering practices which are common today.

- Black Hole Exploits
- False Majority Bullying
- Mass Marketing Through Bots
- Information Gathering Tactics
- Account Theft

Black Hole Exploits

Following image links, or even website suggested links, can be a normal part of most user's day. A friend send a link and suggests checking out an article about a shared interest, upon clicking the browser seems to lag as a url shortener takes 20 seconds to load the correct webpage and eventually you land on the website. Days later you receive statements about unusual login attempts or worse, an online account is overdrawn and you are stuck trying to figure out what happened.

Here's what happens: Somewhere a hacker setup a server to act as the url shortener, which collected all of your browser cookies including logins and then deposited you onto the page in question. The hacker then added your cookies to a browser setup to emulate your usage and turned on autologin hoping to get lucky and catch your online banking or other valuable accounts and quickly change the account data including it's associated email account. Chances are this will result in you sending for a password reset which will go the hacker's email account as a delay, and only after you contact an administrator will the problem be sorted out. By that time the hacker will have had time to withdraw money from a bank account, paypal, etc, and while you'll probably be covered by their policy regarding fraud, it may take up to a month to get reimbursed.

How to reduce the likelihood of such an attack. Have one browser that never touches your online banking, and use it for your social media. Otherwise delete cookies constantly, and even then, use system cleaners to get rid of cookies the browser doesn't delete.

False Majority Bullying

Social media accounts are easy to build or purchase in bulk. It should come as no surprise that just as mass marketers use dozens or even hundreds of accounts to spread a message and try to fool the metrics to look successful, online trolls and even activist groups use the same tactics

to appear popular. If one user attacks you for your political views, you are either dealing with a troll, or someone who is far too eager to argue. But when suddenly you are dealing with dozens or hundreds of combative people on Facebook or Twitter, it causes a scene and can get multiple people banned.

Here is what happens: Someone getting paid to influence a metric (like a liberal hashtag appearing to suddenly emerge online) shifts a written script to include that hashtag and hundreds of accounts start tweeting about it in short bursts using mentions to attract more retweets. After this goes on for a few hours more fake accounts seem to suddenly join and even get combative towards people who respond less favorably. Paid trolling and mass marketing are so similar one only needs to see it in action once to recognize that it is in no way organic. People who cause hashtag to trend organically without paying, usually do so in a matter of days of discussion about a popular topic, like a new movie upon release. Hundreds of thousands of people don't suddenly all agree to argue about 60% of the nonsensical activism related hashtags you see on twitter, however it can happen on occasion. The rest of the time it is paid propaganda, and sleight of hand.

What you can do about it, block and report every single user who bullies as they begin and use the #security hashtags to suggest what you think is happening.

Mass Marketing Through Bots

Not unlike what we just discussed, but a bit more sophisticated perhaps. Targeted marketing through searches can be tedious, but when it's automated it looks like anyone who mentions a product suddenly causes a link sharing fairy to magically respond with either an amazon link, or one to another site which may or may not still exist. I've clicked that bait once or twice myself only to land on 404 pages and realize the scripted bot that sent me the link simply has never stopped doing what it was told.

Here is what happens: One person followed a tutorial and built a bot to sell his or her products and has since given up.

What can you do about it? Not much, just block or ignore it.

Information Gathering Tactics

On Sunday someone you don't know asks if your real name is your account name. They may stick around and make small talk, being complimentary to a point before leaving in a hurry. On Tuesday another person asks for a link to your Facebook to follow you there as well, or asks you to follow them there. This will persist for weeks until one of these accounts get a glance at your Facebook page where they will likely find more info like the state you live in etc. Such information goes into a contact list with countless others who will all be targeted by telemarketers, email spammers, online offers through social media, etc. This attack vector gets creepier when you realize the telemarketing angle is often simply to fill in the blanks by asking a question just to fish for information. Example, "Does John still live there?" - No one named John has ever lived there, and the attacker is aware of that likelihood. They may ask follow ups like, "To whom am I speaking then, so I can make a note of that to prevent future calls for John?" If you give this information you are now on the list for future calls from phony credit card

companies, collection agencies etc. Recently even saying the word yes has been discouraged over the phone, as a recording of it may be used to convince a bank that they are dealing with the actual customer rather than an imposter.

Here is how it happens: Agencies in poorer countries use calling centers to build lead databases as a primary source of revenue. They'll sell that data to as many people and companies as possible to maximize their profits, and couldn't care less how that data is used.

What can you do about it? Just knowing to be cautious how you speak to unsolicited callers helps, but online, be especially careful what you tell strangers about your identity.

Account Theft

There are several ways this happens. Clicking the wrong link, Trusting the wrong person with login credentials, giving certain company apps permissions to make account changes, and others. One day you wake up and realize you have somehow posted 10000 game requests to all of your family and friends, and are locked out of your account. (Well, maybe not locked out, but that is a common claim brought on by shame.)

How it happens: Accepting game requests and allowing apps to post in exchange for virtual livestock was a good example. Another is just plain misuse of API's by some app developers who can let data leak in a variety of ways.

How to prevent it... Change app permissions to reflect your preferences within 30 minutes of creating an account. It may not keep the company from spamming your friends, but at least it won't look like you were doing it.

Conclusion

As a certified: Ethical hacker, Linux system administrator, and programmer in over 7 languages, I can confidently say that these are "low level exploits" which can/should be avoided with cautious practice. This article should in no way infer that by simply following the advice suggested you wouldn't still be vulnerable to higher level exploits. We advise the use of up to date operating systems and reasonable security settings on all browsers, ssh servers, firewalls, etc. If you have privacy concerns you may opt for vpn usage to enhance your privacy, and of course check back frequently for updates about this and other topics.