NASSAU COUNTY
SPiN
A Crime Prevention Partnership
SECURITY / POLICE INFORMATION NETWORK

EDWARD P. MANGANO
County Executive

THOMAS V. DALE
Commissioner of Police

# Social Media Security Threats

### 1. Social Networking Sites

Sometimes hackers go right to the source, injecting malicious code into a social networking site, including inside advertisements and via third-party apps. On Twitter, shortened URLs (popular due to the 140-character tweet limit) can be used to trick users into visiting malicious sites that can extract personal information. Twitter is especially vulnerable to this method because it's easy to retweet a post so that it eventually could be seen by hundreds of thousands of people.

### 2. Social Engineering

A favorite of smooth-talking scammers everywhere, social engineering has been around since before computer networks. But the rise of the Internet made it easier for scammers and con artists to find potential victims.

Social media has taken this threat to a new level for two reasons: 1) People are more willing than ever to share personal information about themselves, and 2) Social media platforms encourage a dangerous level of assumed trust. From there it's a short step to telling your “new friend” about your company's secret project, your new friend might be able to “help” you with that project if you would only give him a password to gain access to a file on your corporate network.

### 3. Mobile Applications

The rise of social media is inextricably linked with the revolution in mobile computing, which has spawned a huge industry in mobile application development. Naturally, people typically download dozens of applications.

Sometimes people download more than they bargained for. In early March, Google removed from its Android Market more than 60 applications carrying malicious software. Some of the malware was designed to reveal the user's private information to a third party, replicate itself on other devices, and destroy user data or even impersonate the device owner.

### 4. Advanced Persistent Threats

One of the key elements of advanced persistent threats (APT) is the gathering of intelligence of persons of interest, for which social networks can be a treasure for that data. Perpetrators of APT's use this information to further their threats, placing more intelligence gathering, and then gaining access to sensitive systems to place their malwares, trojans, etc.

### 5. Impersonation

Several impersonators have gathered hundreds and thousands of followers on Twitter and then embarrassed the people they impersonate, or perhaps worse. Twitter will now shut down impersonators attempting to smear their victims, but only at their own discretion.

### 6. Trust

The common thread across almost all of these threats is the tremendous amount of trust users have in these social applications. Like email, when it hit the mainstream, or instant messaging when it became ubiquitous, people trust links, pictures, videos and executables when they come from "friends," until they get scammed a few times. Social applications have not tricked enough people just yet. The difference with social networks is that the entire purpose of them is to share information, which will result in steeper learning curves for users. Thus, meaning that people will be getting scammed even more.

### 7. Cross-Site Request Forgery (CSRF)

While it isn't a specific kind of threat, but more like a technique used to spread a sophisticated social networking worm, CSRF attacks exploit the trust that a social networking application has in a logged-in user's browser. So as long as the social network application isn't checking the referrer header, it's easy for an attack to "share" an image in a user's event stream that other users might click on to catch or spread the attack.