2d Lt James Marvin

CTC 9

Email is one of the most common delivery mechanisms for network-based attacks. In the early days of social engineering there was the email from the prince of Nigeria who needed your bank account number, so he can transfer money out of his country with a promise of giving you a cut. This might seem on the surface to be ridiculous but in every hay stack there are a few gullible needles. As people gain more experience on the internet, they are less likely to fall for these schemes. This necessitates that hackers craft more believable messages. An excellent source of content for these messages is your social media presence. Your social media feeds provide context and legitimacy that a stranger wouldn’t have been able to get remotely otherwise. The paper by Brown and his colleagues shows that spam emails falsifying social media notifications have a higher click through rate and a better chance of slipping past robust email spam filters [1]. Their results indicated that 85 percent of users who have publicly visible profiles could be targeted easily with a context aware spam attack [1]. The other paper I reviewed demonstrated how attackers can spoof HTTP sessions with your social media provider, so they can extract your personal information and the information of your friends [2].

The key to defense in these situations is to limit the personally identifiable information you put on these sites and avoid displaying it on your profile where possible [1]. One of the most common mistakes is putting your email address on your profile. Even more egregious would be to put your work email on your profile. Besides things the individual can do, social media sites could convert personal information displayed on the site to images making it harder to parse them from the website data. This can be undone by complex OCR software, but nonetheless is a useful hurdle [1]. The general strategy I would propose security minded individuals is to look for ways to decrease their footprint as much as possible in order to limit the contextual information you give to hackers.

Sources:

1. Brown, G., Howe, T., Ihbe, M., Prakash, A., & Borders, K. (2008, November). Social networks and context-aware spam. In Proceedings of the 2008 ACM conference on Computer supported cooperative work (pp. 403-412). ACM.
2. Huber, M., Mulazzani, M., Weippl, E., Kitzler, G., & Goluch, S. (2011). Friend-in-the-middle attacks: Exploiting social networking sites for spam. IEEE Internet Computing, 15(3), 28-34.