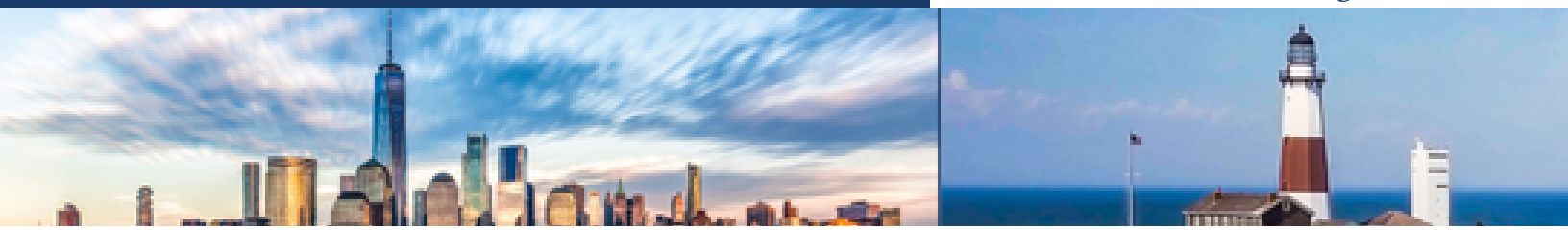
CYBERSECURITY LAW ALERT

August 17, 2023

By: Andrew T. Garbarino, Esq.

RUSKIN MOSCOU FALTISCHEK P.C.

Smart Counsel. Straight Talk.



Get Ahead of the Latest Social Media Attack Now

In what should be a major news story, a large number of LinkedIn accounts appear to have been hacked over the past few months, with some victims being coerced into paying ransom to regain access and control of their own accounts.

The delay in reporting may owe to the fact that the evidence of the hack is gleaned from an uptick – a very large uptick – in requests for help on LinkedIn forums. That noted, one news item explaining the situation may be found here.

While the hacking of a LinkedIn account may seem inconsequential when compared to a banking, hospital or government hacking incident, consider the damage that a person might suffer if a rogue actor were to gain control over your LinkedIn account if they were to post insulting or otherwise damaging content to clients, referral sources, colleagues and employers.

The reputational harm might be devastating.

It appears that these hackers are gaining access by way of ***brute force*** attacks – a traditional hacking method that works by bombarding an account with potential passwords, often using software. While there are a number of permutations, in its simplest form a brute force attack involves hundreds, perhaps thousands, of commonly used passwords – think “pa$$word123” – that are attempted on an account until access is granted.

Other brute-force methods involve the use of previously-stolen passwords on other accounts owned by the same user.

The best protection against these types of attacks is password security. While the mere mention of password security often results in eye-rolling and frustration, it has become a completely necessary aspect of our collective business and personal lives. A good password manager solution can help (but be sure to research, and even speak with your technology consultant, before implementing one).

As to LinkedIn specifically, please be sure to enable your two-factor authentication. Any of you who need help can ask your internal or external tech folks for an assist. It takes less than two minutes and will instantly let you know if someone tries to log into your account from a new device.

For more information, please contact:

Andrew T. Garbarino, Esq.
516.663.6632
agarbarino@rmfpc.com