
**November 27, 2018**

## Cyber Alert – What a Famous Hip-Hop Artist Can Teach About Cyber Security

**Risk Management Question:** The title of this Alert is not merely click bait; it's a real life lesson about cyber security risks and how not to handle them. The fact that it involves a famous hip-hop artist should hopefully get your attention even if you don't listen to his music, are not a fan, or know anything about hip-hop.

**The Issues:** Below is a link to a short article from *CyberVista*, which addresses 3 data security issues stemming from Kanye West's recent trip to the White House. To quote the blog: "If you're ever unsure about how to handle a security issue, you can always just ask yourself: "WWYD – What Would Yeezus Do?" Then do the opposite.

The first issue involves something that has been harped on in the past – the need for strong, complex passwords, which are not used to log into more than one application or site. The camera crews in the Oval Office captured Kanye unlocking his iPhone and revealed his password. It was neither strong nor complex and could be easily guessed by a hacker, even if it had not been captured by the camera crew.

The second issue involves the risk of "shoulder surfing," which involves exposing your password, the content of your email or work while you are "on the go." This is exactly what the photographers in the White House were doing when they surreptitiously caught a peak at Kanye's iPhone password. Always assume that anyone sitting behind you on a plane or train may look at your screen.

The third issue involves your social media activity – Kanye is infamous for his provocative social media posts and outbursts. It's a helpful reminder that hackers will crawl the personal information you post on social media to use in phishing or social engineering exploits against you, someone else at the firm or another family member. So be careful on social media and be smart about your posts – try to not provide information that can be used by hackers.

**Risk Management Solutions**:

Create strong passwords:

- It's been said before but is worth repeating – the use of strong passwords is arguably the single most critical component of a successful cyber security strategy. Increasing the length of a complex password from 8 to 12 characters exponentially increases the time to hack a password.

- A complex password should include a mix of upper and lower case letters, numbers, symbols and special characters.

- Alternatively, you could use a "passphrase" – a string of several random words that is easy to remember – to secure your accounts and devices.

NIST has changed its guidance on passwords, preferring lengthening and strengthening them over frequently changing them, but be sure to comply with any outside counsel guidelines on passwords that specify how frequently they are to be changed.

Beware of shoulder surfers:

- Just because you are not famous does not mean you are safe from snoopers – innocent or malicious. Portable devices are ubiquitous, with more and more employees using them to do work outside the office.

- When you are out in public, be aware of your surroundings and the people around you at all times. Don't be that person on the train or airplane that allows other to see what you are doing or your communications.

- Consider using a privacy screen on your device when available. They come in different shapes and sizes but all are basically designed to reduce your screen's visibility at an angled view, making it more difficult for other people to see your device.

Don't Overshare on Social Media:

- Threat actors can gather personal information from your online profiles – such as contact information and location records – that can be used to conduct a cyber attack. You need to be very conscious of the information that you are putting out publicly on the internet.

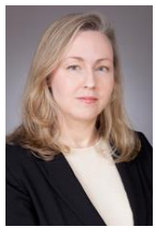
- If you are unsure of whether to post something on social media, leave it out.

To paraphrase a Miranda warning, your contact information and location data on your mobile devices can and eventually will be used against you. So check the settings on your devices and be careful out there. Here's a link to the article referenced above.


Steven M. Puiszis
312-704-3244
spuiszis@hinshawlaw.com

Anthony E. Davis
212-471-1100
adavis@hinshawlaw.com

Noah D. Fiedler
414-225-4805
nfiedler@hinshawlaw.com



Annmarie D'Amour
212-471-6231
adamour@hinshawlaw.com