Common Threats

Kevin Mitnick, Chief Hacking Officer at KnowBe4, explores three common social engineering threats.

USB Attack

- Almost 50% of USB flash drives randomly distributed on a major university campus were plugged in and had files opened.
- Bad guys typically mail or physically distribute USB flash drives to their targets and can install trojans to gain control of your system without you opening any files.

Kevin Says

Only connect USB devices that are given to you by someone you know and that you expect.

Fake Login

- Over 81% of recent data breaches have been caused by weak or stolen passwords.
- Bad guys register fake domains and set them up to look just like legitimate sites. Then they send phishing emails to trick you into going to the fake site and entering your username and password.

Kevin Says

Be very suspicious of any requests you receive that ask you to enter your username and password.

Malicious Download Attack

- Almost 14 million new phishing sites are created each month.
- Bad guys host hacked versions of legitimate software (in this case, meeting software), that once installed, give them a tunnel into your organization's network.

Kevin Says

Don't trust links for software received through text messages or emails. Directly open the legitimate website and download the file from there.

STOP
before plugging any external media into your computer.

LOOK
before you click a suspicious link.

THINK
before downloading any software.

KnowBe4