USB keys will end you

If it's too good to be true, it's too good to be true...

Elburz Sorkhabi
Sep 6 ♡1

Problem

Hackers realize you're getting savvy about online attacks *and* that you love free things. This results in a crafty technique called a USB Drop Attack. Hackers will drop USB keys loaded with malware or malicious software on the ground outside offices or in public places. You pick up the USB key thinking it's your lucky day, you plug it into your computer, and that might just be enough to compromise your system. A 2016 study found that 98% of USB keys dropped around a university campus were picked up and 45% of the USB keys had at least 1 file opened by the user who plugged them in. That's a 45-98% rate of success on these attacks...that's bats**t crazy.

High-level solution

The reality of the situation is there are so many variations and levels of complexity to USB drop attacks that there is no single way to secure your system against them. Some of them have malicious files that lure you into opening them, such as *passwords.pdf*. Others simulate keyboard commands to exploit your system, like the RubberDucky used in Mr. Robot. And there are even $60 USB keys that use an electrical exploit to fry your computer. This is why many corporate environments just straight up disable USB ports on their computers.

Recommendation

Do. *Not*. Pick. *Up*. USB. *Keys*. Anywhere.

Not off the street. Not in the lobby of your office. Not in the break room. Nowhere. If it's not yours, just leave it. Simple! This is the only way to avoid USB Drop Attacks. If you need a USB key for work or your home life, they are extremely affordable and come in many form factors and styles. Here's a few recommendations:

1) Small form factor: Samsung USB 3.0 Flash Drive Fit - 32GB for $9

Samsung USB

2) Affordable with lots of storage: Kingston Digital Data Traveler SE9 G2 USB 3.0 Flash Drive - 64GB for $13

Kingston USB