PROTECT YOUR DATA!

Thumb Drives Are Evil!

By: Karl Demuth
Director of Information Technology
Wichert Insurance
www.wichert.com

keep this guy out of your personal data

Thumb drives can be:

- A Crutch
- Clever
- Cute
- Destructive

Recently we obliged a Request for Proposal that stated we must submit our proposal via a thumb drive. Ok. We bought a new thumb drive, wrote our information onto it, and submitted it. Short of that, I cannot see much reason most of us would need to use a thumb drive for business.

Here is the problem... thumb drives can and have been used as vectors of entry for malware, spyware, and ransomware. Their use for this is incredibly successful. Unfortunately, it is our own curiosity that makes the scheme successful.

Scenario #1:
You arrive at work and find a thumb drive lying in the parking lot. Curious, you pick it up, carry it to your desk, and stick it in your computer to find out what is on it.

Here is what really happened:
A hacker left the thumb drive in the parking lot. When you put it in your computer it installed spyware onto your computer and now the hacker can control your computer while you are away in the evening. There were no warning signs or errors and you may never know the spyware was installed or that private customer information was lost.

Scenario #2:
You are at a conference and a vendor has a bowl of thumb drives sitting at their booth. You pick one up, knowing it has some advertising on it, but also knowing you can use it later to store family pictures or your next presentation.

Here is what really happened:
A hacker plucked the same thumb drive from the bowl earlier in the day, went back to a hotel room, wrote ransomware onto the thumb drive, and returned it to the bowl, completely unbeknownst to the booth vendor or you. When you put the thumb drive into your computer, the hacker wins.
Ransomware is installed from the thumb drive onto your computer, encrypting all your files and demanding payment to recover them; meanwhile it spread across our network to other computers.

Scenario #3:
You find a thumb drive in the office near the copier or maybe on your desk. "Hmm... who does this belong to?" You put it in your computer...

Here is what really happened:
A hacker, posing as a cleaning person, a vendor, a customer, your coworker's teenager, or who-knows-what, left the thumb drive there. You know the rest of the story.

In conclusion:
I suggest not using thumb drives. If you must use one to save an RFP or a presentation, buy a brand new thumb drive and do not let it out of your possession. If you find one and do not know from where it came, throw it away. Do not be curious. If you are that curious, take it home and put it in your own computer!