# Without safeguards, smart home can be a dumb choice, expert says

May 6 2014

Credit: Peter Griffin/Public Domain

Smart technology can perform all sorts of tasks in our homes. Turn on our lights. Unlock our doors. Crank up our thermostats. And quite possibly, give someone access to our valuables or our bank accounts.

The rise of smart technology worries cyber security expert Jerry Irvine, who believes many homeowners are unknowingly trading security for

convenience when they install smart gadgets or systems in their homes.

"You should be concerned enough not to do it, or to pay somebody to do it for you correctly," said Irvine, who is chief information officer and a partner with Prescient Solutions, an information technology company in suburban Chicago.

"It's not the technology that's the problem," he said. "It's the way people are using it."

Smart technology lets users control a number of functions remotely from a computer, tablet or smartphone. Typically the users connect to those systems via an Internet site, and almost always the systems can be controlled wirelessly.

Unfortunately, those systems are often insecure, Irvine said. And that vulnerability can open the door - literally or figuratively - to people who are looking to steal from you.

Let's say you have a smart thermostat. It operates via a chip that has no security protection, Irvine said, so a hacker could use it as an entry point to get access to your computer. If that computer isn't adequately protected with antivirus software and its operating system isn't updated regularly, he said, the hacker can get in fairly easily and find information that will let him or her withdraw money from your bank accounts, charge items to your credit cards or otherwise wreak havoc with your finances.

If you think that can't happen, consider this: It appears the hackers who ransacked Target's computer system got in via the heating, ventilation and air conditioning system, said Irvine, who serves on the National Cyber Security Task Force, a body that advises federal decision makers on cyber security policy.

Hacking into a smart system can give someone physical access to your home, too. A thief could disable your security alarm, turn off security cameras and even unlock the smart lock on your door, Irvine said.

What makes these systems even more problematic is they're often controlled by smartphones, which Irvine called "the most insecure device we have." Most users don't even have them set up to require a personal identification number for access, he said.

How can you keep hackers out? If you want to use smart technology, Irvine said, put those controls on their own virtual local area network, or VLAN - a network that's different from the one used for your personal computer and other devices. Configure that VLAN so a person can communicate with the devices on it only through an encrypted virtual private network, or VPN.

That's beyond the capability of the average homeowner, Irvine said, but you can hire a computer technician to do the work for you. It should take about an hour and cost maybe $75, he said.

Have the technician show you how to change the encryption key - the password that decodes the information on the network - after he or she leaves, he advised. That way, the technician won't have access to your network, either.

Irvine said cloud-based home security solutions are an option, but those could still be hacked if you're not careful. He suggested using a unique user name just for that account, something that's hard for a hacker to guess and that's not your email address. You should also use a unique password that's 10 to 15 characters long and includes both capital and lower-case letters and at least one number and one special character - that is, a punctuation mark or symbol such as a percentage sign.

In fact, those user name and password precautions are wise for all your online transactions. Irvine also recommends making online payments only with a low-limit credit card and never allowing a website to save your credit card information.

Never make an online payment with a debit card or a direct transfer from your bank account, he said. At least you have protections if you pay by credit card. If your bank account is compromised, the loss is yours.

That's using technology in a smart way.