Trusted electronic hardware: Top 10 list of what consumers trust most

August 20 2015, by Krista Burns

Credit: Carnegie Mellon University Electrical and Computer Engineering

Society puts a lot of trust in its electronic devices. Whether following a GPS to the beach or paying a bill online, consumers rely on their electronics for everyday tasks.

A new survey conducted by the College of Engineering at Carnegie

Mellon University asked 2,000 U.S. consumers to rank the 10 [electronic devices](#) that users trust most with their personal information:

Top 10 ranking of devices users trust most

1. Home phone
2. Home security system
3. Fitness device
4. Car electronics
5. GPS device
6. Smart watch
7. Cell phone
8. Desktop computer
9. Laptop computer
10. Tablet

Items in the home are at the top of the ranking. When it comes to concerns about their [personal information](#) being at risk through hacking, the survey showed that users are most concerned about their laptop computer (54.3%), desktop computer (49.3%) and smart phone (48.2%) becoming victim of malicious activity.

However, there are differences among men and women. Men are more likely to trust their [car electronics](#) (53.8%), GPS devices (53.7%) and smartphones (53.5%), while women are more likely to trust their [home security](#) systems (50.5%), cell phones (50.1%) and smart watches (49.8%). The data also shows that users ages 18-24 are more prone to put their trust in a smartphone, compared to older users. On average, users trust their personal devices just as much as their work devices.

Of all plug-ins available (devices that were not part of the initial electronic device purchase), users trust the following items the most:

1. Headphones (73.4%)
2. Mouse (70.7%)
3. Speakers (70.6%)
4. Power charger (69.2%)
5. DVD (61.5%)

This survey was conducted to gain insight into consumers' trust levels regarding electronic device hardware. Researchers in Carnegie Mellon's College of Engineering are training the people and developing the technology needed to combat hardware security threats. Ken Mai, a senior systems scientist in the [email=kristab@cmu.edu]electrical and computer engineering department[/email], is creating new, low-cost, hardware-level methods of securing electronic systems against malicious activity and counterfeiting.

PHYS.ORG

TRUSTED HARDWARE

WHAT DEVICES DO USERS TRUST THE MOST?

TOP 10 LIST

01 HOME PHONE

02 HOME SECURITY SYSTEM

03 FITNESS DEVICE

04 CAR ELECTRONICS

05 GPS DEVICE

06 SMART WATCH

07 CELL PHONE

08 DESKTOP COMPUTER

09 LAPTOP COMPUTER

10 TABLET

Carnegie Mellon University
College of Engineering
engineering.cmu.edu

"When users think about the security of their electronics, most are concerned with their software and the Internet," says Ken Mai, a senior systems scientist in the electrical and computer engineering department. "But it's critical that users consider the security of their hardware too. Security vulnerabilities in hardware can be just as dangerous (if not more so) as software breaches, and are usually much harder to fix."

Mai and the College of Engineering have a unique angle for approaching the topic. "We saw an opportunity to approach hardware security from a hardware design perspective versus a security perspective," said Mai. "Most of the people working in the space are security people trying to do hardware. We are hardware people applying our skill set to provide security."

Provided by Carnegie Mellon University Electrical and Computer Engineering