Would you notice if your calculator lied to you? The research says probably not

November 1 2019, by Monica Whitty

Credit: AI-generated image (disclaimer)

These days, it's hard to know whom to trust online, and how to discern genuine content from fakery.

Some degree of trust in our devices is necessary, if we're to embrace the growing number of technologies that could potentially enhance our lives.

How many of us, however, bother trying to confirm the truth, and how many blindly approach their online communications?

In a study published this week, Texas Tech University researchers tested how university students reacted when unknowingly given incorrect calculator outputs. Some students were presented with an onscreen calculator that was programmed to give the wrong answers, whereas a second group was given a properly functioning calculator.

Participants could also opt not to use the calculator, but most chose to use it—even if they had good numeracy skills. Researchers found most participants raised few or no suspicions when presented with wrong answers, until the answers were quite wrong. In addition, those with higher numeracy skills were, unsurprisingly, more suspicious of incorrect answers than others.

Do the math

To understand these results, we need to acknowledge calculators were created to make our lives easier, by reducing our mental burden. Also, there were no real consequences for participants who did not realize they were being duped.

Perhaps if they were completing their income tax forms, or applying for a loan, they may have been more thorough in checking their results. More importantly, there's no reason an individual ought to feel suspicious about a calculator, so the participants were acting in accord with what we might expect.

People can't spend their time deciding if they should trust every tool they use. This would consume too much time and energy. This study, however, was carried out with university students in a lab. What are the consequences of this in the real world, when much more is at stake?

The Internet and digital technologies have changed our lives for the better in so many ways. We can access information at super speeds, communicate regularly (and in fun ways) with our friends and family, and carry out mundane tasks such as banking and shopping with ease.

However, new technologies pose new challenges. Is the person you're talking to online a real person or a bot? Are you developing a real romantic relationship on your dating app, or being conned in a romance scam?

To what extent do people blindly accept their technologies are safe, and that everyone online is who they claim to be?

Hackers are often phishing for data

The Internet of Things is already changing our lives in and outside the home. At home, there's the constant threat that we're being listened to and watched through our devices. In August, Apple publicly apologized for allowing contractors to listen to voice recordings of Siri users.

Similarly, as autonomous vehicles become the norm, they too pose ethical concerns. Not only do we need to be worried about the programmed moral choices on whom to harm if an accident becomes inevitable, but also whether criminals can hack into these vehicles and alter programmed decisions.

Also, there have been reports of benign-looking USB cables being rigged with small WiFi-enabled implants which, when plugged into a computer, let a nearby hacker run commands. We even need to think about the safety of health devices, such as pacemakers, which can now be hacked.

A major problem organizations and governments are trying to solve is stopping individuals from falling victim to phishing. A phish is an email

or text which is made to appear authentic and trustworthy, but isn't.

Cybercriminals use them to trick users into revealing secret information, such as bank account details, or clicking on a link that downloads malicious software onto their computer. This software can then steal passwords and other important personal data.

Clicking on a phishing message can have long-lasting detrimental effects on an individual or an organization, as was the case with an Australian National University data breach last year.

We're yet to effectively train people to recognize a phish. This is partly because because they're often realistic and difficult to identify. However, it's also because, as illustrated in the Texas Tech University study, people tend to place undue trust in technology and devices, without pausing to check the facts.

Knowledge is power, and safety

It's incredibly difficult to have the right balance between skepticism and trust in the digital age. Individuals need to function in the world, and the mental effort required to constantly check all information is perhaps more than what we can expect of people.

That said, one positive takeaway from the calculator study is that training is critical if we want to improve people's cybersecurity practices. This includes training individuals on what to do as online users, how to do it, and why it's important.

As with all learning, this needs to be repetitive and the individual needs to be motivated to learn. Without effective learning methods, end-users, organizations, and state nations will remain vulnerable to cybercriminals.