The Perils of Internet Interactions

W. Clark Akers

Marymount University

Abstract

Throughout the internet there are plenty of scams and opportunities for you to give out information you never intended to share. This paper investigated the many ways that humans misuse of the internet is the cause of most of the issues found on the internet. It’s not from hardware or software problems but from human error. Trust is thought of as an absolute yet when cyber security is involved no one is trustworthy enough to handle your personal information.

Keywords

* Trustworthiness - the ability to be relied on as honest or truthful
* Misinformation - false or inaccurate information, especially that which is deliberately intended to deceive.
* Distrust and verify (yes two words but necessary)- use evidence and experience to verify before you willing information give out information

The Perils of Internet Interactions

In the modern age everything seems to be online, from shopping to school people are able to live more and more of their lives through the internet. Modern tools like social media and online profiles have normalized displaying more and more information openly out on the internet. The benefit to this is ore streamline services and methods of payment but at what cost? This all stems from a sense of security or trust in a system that is basically non-existent on the internet.

“The allusion of information can be more dangerous than ignorance” (Botsman 2018) this speaks to heart of the problem with basic human cybersecurity on the internet. People who ignore certain pop ups and phishing emails normally never have to deal with cyber security issues. The problems arise when people fall for these scams and get themselves in all sorts of problems. But who’s to blame them nowadays everything seems so real. To combat the growing stigma of needing to trust different sources on the internet even scammers are getting smarter. They not only give you the information you want to hear they also try to use fake methods to gain trust like saying the pop up is from reputable sources like Apple or Google.

Using well known trusted sources is a newer tool of scammers yet targets one of the most basic methods of trust that society has built. Which like Mrs. Botsman discussed and labeled as “Institutional” (Botsman 2018) trust, which has developed as companies and services become part of everyday life. For example, Uber, we as a society have put trust in this company that they will provide safe and trustworthy drivers to provide rides for a fee. Yet there have been multiple instances of Uber drivers being extremely unqualified and even criminals in some cases. Mrs. Botsman discusses one such instance where an Uber driver was completing rides in between murdering people. Uber claimed they had no idea there was any chance he was a serial killer and even said his Uber rating were very high. Although this seems to shift the blame from Uber this asks a bigger question of what information validates trust for a random individual?

Humans are taught from a young age to trust institutions like schools and government as absolute authority, what they say goes. Yet in a world of ever evolving scammers and digital information how do we know that the information provided to these institutions is credible? As this digital age continues to revolve new steps to ensure your trust is well placed. One such method is to trust “proportionally to the level of risk” (Singer 2019) which means simply to asses even the most trusted sources when information is requested to weigh the risk of consequences of giving out the required information. This could include anything from social security numbers to even as simply as entering your email address. Any of this information can be used as a first step towards using your information in ways you didn’t allow.

Internet users are taught at a young age about internet scams, it sees to pop up in every day culture. There’s a running joke about interne scams that pokes fun at the common scam of sending money to an international person of royalty who just needs your money to get access to their “Large Estate”. Though this seems like an obvious scam many people have fallen under the scams enticing spell. This simple scam is a small example of the problem with trusting if anyone is who they say they are on the internet.

Although understanding of the internet and what you can do on it is becoming greater and greater as a whole most people don’t understand cyber security at even its most basic level. The general risk of even going on the internet becomes more and more dangerous yet more and more people are using the internet every day. This is the start to an internet epidemic that hasn’t even begun to be understood.

A very recent subject of internet fame came from a Netflix documentary called “Don’t F\*\*k with Cats” which is an investigative documentary about how multiple internet groups helped catch one of Canada’s most notorious killers. This killers name was Luke Magnotta, posted multiple videos of him killing and glittering cats until it ultimately turned into a human victim. Magnotta who grew created a very extensive fake web of information about himself used the internet as his main form of misinformation. He flooded the internet with edited pictures and profiles of himself as being a model and having numerous famous connections. As these internet investigators continued to add evidence to their theory of connecting him to the crime. People who knew him described his use of the profile as a way to “reinvent himself” (Bruney 2019) which seems harmless but when you look at the bigger picture provided him ample opportunities to capitalize on his misinformation. He used locations and fake pictures to make it difficult for anyone to pinpoint exactly where he was.

There are two different sides to cyber security shown through this documentary. The first being the obvious use of misinformation by Magnotta to display a more desired version of himself to others. The second being that people who know how to use the internet and its many functions can find a dangerous amount of information against you. The internet investigators in this film weren’t cops or law enforce the of any kind, they were internet junkies who collectively found the awful stuff Magnotta was posting and decided to do something about it. Although it’s shown in a positive light it shows a true view of how much even the common man can find about you just using a computer.

This all boils down to Mrs. Botsman’s point of “information is the currency of interactions” (Botsman 2019) nowadays everyone inaction count on average is way higher than ever before in human history and that is all due to the internet. No one needs to even leave their house to have an interaction anymore it can be done through social media outlets and even through calls and texts. The increase in interactions only continues to create a more dangerous environment for humans to try to navigate.

References

Botsman, R. (Director). (2019, April 4). *The Biggest Issue in Cyber Security is Humans, Not Machines* [Video file]. Retrieved September 13, 2020, from https://www.youtube.com/watch?v=15lS2SfW4pM

Bruney, G. (2020, August 20). Netflix's 'Don't F\*\*k With Cats' Tells the True Story of One of Canada's Most Infamous Murderers. Retrieved September 13, 2020, from https://www.esquire.com/entertainment/a30308038/netflix-dont-fuck-with-cats-luka-magnotta/

Singer, A. (2019, May 17). The 3 Cybersecurity Rules of Trust. Retrieved September 12, 2020, from https://www.darkreading.com/perimeter/the-3-cybersecurity-rules-of-trust-/a/d-id/1334732