SCHOLARS
STRATEGY NETWORK

How to Safeguard against Digital Victimization

Kyshawn ('Shawn) Smith, Radford University

Now more than ever, social existence is defined by both physical and digital reality. Nearly everything one can experience in a physical respect can also be experienced online, and sometimes in more profoundly significant ways. Experiencing victimization is no exception. Moreover, as demonstrated by such watershed events as the 2016 Wells Fargo scandal – where a few million customers had accounts opened fraudulently in their name by the international banking conglomerate – the presumptive gatekeepers of user security in the digital world too often fall short in providing effective safeguards against such calamities.

Undergirding these failures lie misunderstandings about the distinctions in victimization experienced between digital and physical spaces. For instance, far more in the digital world, people communicate, buy and sell goods and services, harm one another other, and experience countless other interactions all without any direct physical contact. While digital victimization runs the gamut of offenses prevalent in the physical world, it is often discussed, understood, and addressed differently by crime scholars because the offenses are committed without the victim and offender ever physically interacting (e.g., harassment, sexual solicitations, stalking).

Yet, digital and physical victimization are not entirely different. Rather, the digital world can and should be understood as an extension of the physical world – and thus digital victimization should be understood in a similar light. With this in mind, methods for understanding such predatory behavior as harassment and assault in the physical world should be taken into the digital world and inform discussions about how to support victims while deterring perpetrators.

The Victims and Impact of Digital Victimization

Those who fall prey to digital offenses suffer just as much, and in some respects more, than non-digital victims in terms of emotional trauma. And that says nothing of the financial impact of digital victimization, which can be substantial. Between 2010 and 2015, the U.S. Federal Bureau of Investigations averaged just over 288,000 complaints of Internet scams and over one billion dollars in total loss in 2015 alone. In the United Kingdom, reports of credit card theft, purchase of misrepresented products, and solicitation of bank account information (phishing) have all risen by at least 5% from 2003 – 2013 with no indication of a decline anytime soon.

Though not always well-publicized, a good deal is already known about digital victimization. For starters, given the higher concentration of Internet users 34 and under, it's no surprise that most research has shown victims online tend to be young. Unfortunately, this also means that online victims are often less familiar with the dangers of digital spaces, the legal measures available when victimization occurs, and the limitations of such measures. Victims' age can also limit their ability to advocate for themselves.

Online, females are disproportionately targeted by offenders – particularly when the nature of the victimization entails intimate relationship development (i.e., online dating). Offenders intending to manipulate their relationship with a victim tend to be more successful with female targets. This phenomenon is exacerbated by the anonymity the digital world allows.

Linking Digital Victimization and Routine Activities

Significant as these observations are, demographic findings alone only allow for partial understanding of digital victimization. Accordingly, greater interest of late has turned to studying the *routine behaviors* that influence one's vulnerability to cybercrime and other digital victimizations. Stemming from the work of prominent criminologists Lawrence Cohen and Marcus Felson, expanded applications of *routine activities*

theory surmise that criminal activity is more likely to happen when three factors converge:

- ***Weak guardianship*** – when a space has few effective means for preventing, proving, or punishing crime. The anonymity offered by digital spaces coupled with a lack of effective crime prevention measures for digital spaces means fewer disincentives for potential criminals.

- ***The presence of suitable targets*** – spaces with a higher density of susceptible targets are more likely to attract criminals. This feature is particularly prominent in online dating applications and websites, as well as other online connection forums.

- ***The presence of capable offenders motivated to seize criminal opportunities*** – when a space has both weak guardianship and suitable targets, offenders will likely follow shortly behind. The statistics above prove that there are many capable and willing offenders across digital platforms.

Thus, the risk of digital victimization will be higher the more routine (frequent and predictable) one's activities are in a space with the three factors outlined above. In short, an individual's risk of digital victimization increases when their behavior online is easy to observe in public spaces, occurs in a space that obscures the identity of offenders, and offers immediate rewards for the prospective offenders. This increased risk has been observed in offenses like online financial theft in auctions and Internet banking – especially in highly public settings with minimal network security.

Policy Recommendations

Routine activities theory can offer insight on the pervasive problem of digital victimization and help identify new paths towards effective safeguards. To that end, the conversation about victimization should take special note of the fact that the existing safeguards against such victimization are, at least for now, relatively weak.

We must also recognize the heightened vulnerability of young, female audiences and prioritize policy efforts with what is known about the typical digital behaviors of both young people and women. This is not to say that the general public at-large should not be wary of their risk in navigating digital spaces; rather, efforts should simply focus on those who face the greatest risk.

Furthermore, work must be done to destigmatize digital victimization. Too often, digital victims are reluctant to come forward and announce their trauma because of shame, fear, or uncertainty. To move in the right direction, these offenses and the trauma that stems from them can no longer be trivialized. The impact and frequency of digital victimization is often erroneous or underreported because these offenses are trivialized and because cybercrime definitions continue to expand and change. This, in turn, leads to inaccuracies in the documentation of such offenses and causes greater difficulty in implementing proper safeguards.