The difference between cybersecurity and cybercrime, and why it matters

October 19 2017, by Roderick S. Graham

Confidence scams carried out online are still rampant. Credit: R. Stevens/CREST Research, CC BY-NC-SA

A Texas woman in her 50s, let's call her "Amy," met a man online calling himself "Charlie." Amy, who lived in Texas, was in a bad marriage. Charlie said he was a businessman and a Christian, and wooed her. "He was saying all the right things," Amy later told the FBI. "He was interested in me. He was interested in getting to know me better. He was very positive, and I felt like there was a real connection there." Early on,

Charlie told her he was having some problems with his business and needed money. She wanted to help.

From 2014 to 2016, she sent him US$2 million – often in installments of a few thousand dollars at a time, always hoping and expecting to get paid back. After she alerted the FBI, two Nigerian citizens were arrested near Houston – both pleaded guilty to wire fraud charges in connection with Amy's relationship with Charlie. The person who played the character of Charlie has not been identified.

This story is a cautionary example of a crime that happens online. But most advice for avoiding online dangers – like having long passwords, using two-factor authentication and encrypting data – wouldn't have helped Amy.

The crime that befell her has nothing to do with cybersecurity. It's cybercrime, a human-centered crime committed in a digital environment. There are more of these each year: In the U.S. in 2016, 298,728 complainants reported losing more than $1.3 billion in various types of cybercrimes, including romance scams but also involving fraudulent online sales, extortion, violent harassment and impersonation scams, among others. As a social scientist who studies online behavior and as the program coordinator for one of the few cybercrime undergraduate programs in the United States, I find it unfortunate that problems like Amy's get relatively little national attention, especially compared to cybersecurity.

Victims of confidence fraud and romance scams

In 2015, the number of U.S. victims of online confidence fraud, including romance scams, skyrocketed. And in 2016, the number went even higher.
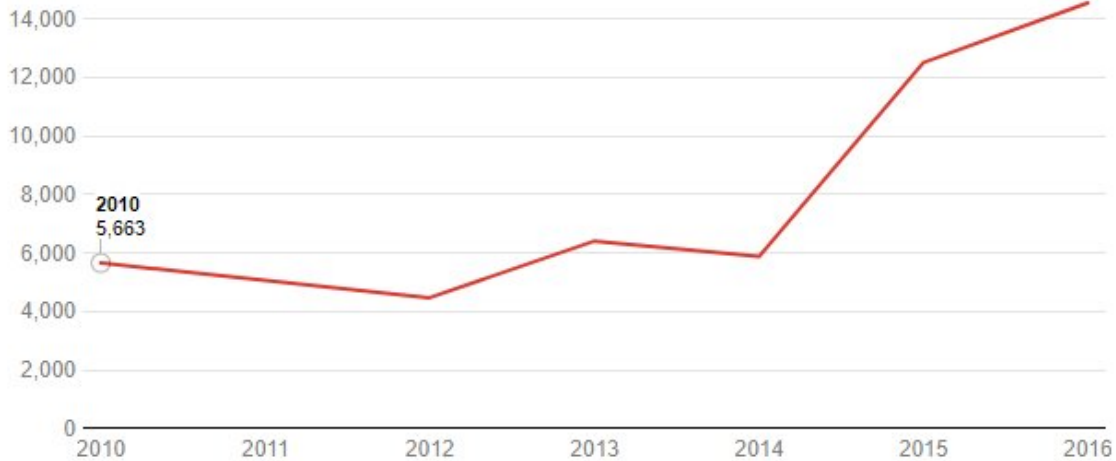
The Conversation, CC-BY-ND

Source: FBI Internet Crime Complaint Center

Understanding the differences

Cybersecurity is not merely a set of guidelines and actions intended to prevent cybercrime. The two types of problems differ substantially in terms of what happens and who the victims are, as well as the academic areas that study them.

Cybersecurity is ultimately about [protecting government and corporate networks](link), seeking to make it difficult for hackers to find and exploit vulnerabilities. [Cybercrime](link), on the other hand, tends to focus more on protecting individuals and families as they navigate online life.

The U.S. has created several initiatives to improve its cybersecurity, including investments in cybersecurity education and expanding efforts of government agencies.

Differences between cybersecurity and cybercrime

	Cybersecurity	Cybercrime
Types of crimes	Crimes where a computer network, software or hardware is the target (ransomware, viruses, worms, SQL injection, distributed denial of service attacks)	Crimes where the human or the human's data is the target (romance scams, cyberbullying, hate speech, sexting, child pornography trafficking, trolling)
Victims	Corporations and governments	Families and individuals
Academic programs	Computer science, computer engineering, information technology	Criminology, psychology, sociology
Intellectual focus	Applied science oriented – coding, networking and engineering strategies for making networks more secure	Basic science oriented – theoretical understandings of how and why crime is committed

The Conversation, CC-BY-ND
Source: Roderick Graham

Unfortunately, upgrading official networks and training future generations of cybersecurity professionals will not necessarily benefit people like Amy. Technical solutions won't solve her problems. Social science research into human behavior online is how to help millions like her learn to protect themselves.

Little research

One of the few studies on [romance scams](#) like the one that ensnared Amy suggests that there are [three stages to these types of cons](#). It starts with the criminal engaging in intense online communications with the victim. In Amy's case, Charlie undoubtedly contacted her repeatedly as their relationship began. That built her trust and lowered her defenses – and commanded much of the time and energy she had for social interaction.

Once the victim is isolated from other interpersonal social experiences, the illusion of connection and interdependence can deepen. Charlie no doubt kept this illusion alive any way he could, taking as much of Amy's money as he could. In the third and final stage, the target finally sees through the veil and learns that it's all been a scam. That's when Amy, urged by her financial advisor, suspected fraud and called the FBI.

More research on [cybercrime](#) could help deepen scholars' and investigators' understandings of how these [social science](#) problems play out online. To my knowledge there are [just](#) [four](#) [cybercrime](#) [programs](#) at residential four-year colleges. With more effort and investment, academics and law enforcement could learn more and work better together to identify and protect the real people who are at risk from these online criminals.

This article was originally published on [The Conversation](#). Read the [original article](#).

Provided by The Conversation