Trends in Phishing Attacks: Suggestions for Future Research

Jeffrey Gainer Proudfoot  
*University of Arizona, jproudfoot@cmi.arizona.edu*

Justin Scott Giboney  
*University of Arizona, jgiboney@cmi.arizona.edu*

Ryan M. Schuetzler  
*University of Arizona, rschuetzler@unomaha.edu*

Alexandra Durcikova  
*University of Arizona, alex@eller.arizona.edu*

Follow this and additional works at: [https://aisel.aisnet.org/amcis2011_submissions](https://aisel.aisnet.org/amcis2011_submissions)

**Recommended Citation**

[https://aisel.aisnet.org/amcis2011_submissions/424](https://aisel.aisnet.org/amcis2011_submissions/424)
Trends in Phishing Attacks: Suggestions for Future Research

Research in Progress

Jeffrey Gainer Proudfoot  
University of Arizona  
jproudfoot@cmi.arizona.edu  

Justin Scott Giboney  
University of Arizona  
jgiboney@cmi.arizona.edu  

Ryan M. Schuetzler  
University of Arizona  
rshuetzler@cmi.arizona.edu  

Alexandra Durcikova  
University of Arizona  
alex@eller.arizona.edu  

ABSTRACT

One of the most common and costly forms of deception and fraud online is phishing. Due to the ramifications of successful phishing attacks, security experts and researchers seek to better understand this phenomenon. Prior phishing research has addressed the “bait” and “hook” components of phishing attacks, the human-computer interaction that takes place as users judge the veracity of phishing emails and websites, and the development of technologies that can aid users in identifying and rejecting these attacks. Despite the extant research on this topic, phishing attacks continue to be successful as tactics evolve, rendering existing research less relevant. Although numerous tools have been created to aid people in recognizing phishing attacks, users disregard the recommendations of these tools. This paper summarizes the core of phishing research, provides an update on trending attack methods, and proposes future research addressing computer credibility in a phishing context.