Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union

Cosima Rughiniş [a,*], Răzvan Rughiniş [b]

[a] University of Bucharest, Schitu Măgureanu 9, Bucharest 010181, Romania
[b] University Politehnica of Bucharest, Splaiul Independenţei 313, Office EF303, Bucharest 060042, Romania

ARTICLE INFO

Article history:
Received 14 September 2013
Received in revised form
5 March 2014
Accepted 20 March 2014

Keywords:
Cyber-security
Cyber-crime
End-users
European Union
Eurobarometer survey
Cluster analysis

ABSTRACT

We use large-scale survey data from the Eurobarometer 77.2/2012 to explore variability in online activity, cyber-crime exposure, and security measures of end-users in European Union (EU27). While cyber-security is a high-priority activity for security experts and researchers, end-users conduct it in the context of their daily lives, as a socially accountable and resource-limited activity. We argue that end-users' security behaviors should be analyzed in relation to their experiences of online victimization, in the context of their routine activities. An ecological analysis at country level indicates that societies with widespread Internet use support cultures of higher cyber-security. They also expose daily Internet users to higher cyber-crime risks, but this positive correlation is weaker, with Romania and Hungary as two notable exceptions of high average exposure with low overall Internet use. Given the negative feedback loops between security responses, exposure to cyber-crime, and online activity, we find that, at individual level, linear causal modeling on survey data is impractical, and we propose classification analysis as a better tool for capturing variability. We use K-means cluster analysis to identify five types of end-users' orientation towards security in the context of their activity: 'explorer', 'reactive', 'prudent', 'lucky', and 'occasional' users, and we discuss their profiles of online activities and experiences. 'Prudent' users are relatively neglected in public campaigns for Internet security. Classification analysis is a productive tool for understanding end-users' security orientations through survey data and for informing public interventions.

Introduction

End-users are primary characters of the scientific literature on cyber-security of recent years. Many pieces of research attempt to measure, illustrate, or explain their low compliance with security rules. There are three main portrayals of end users, accounting for this apparently irrational behavior. There are the 'cognitively lazy' users, operating within a bounded rationality, under heuristics that overvalue present comfort at the expense of protection against future risks. There are also the 'economically rational' users, balancing their own costs

* *Corresponding author*. Tel.: +40 213112168, +40 722953341 (mobile); fax: +40 213158391.
E-mail addresses: cosima.rughinis@gmail.com, cosima.rughinis@sas.unibuc.ro (C. Rughiniş), razvan.rughinis@cs.pub.ro (R. Rughiniş).

http://dx.doi.org/10.1016/j.cose.2014.03.008
0167-4048/

and benefits of security advice and deciding on what appears to security experts as a low level of compliance. Last but not least, there are the 'social' users – also the prototypical victims of social engineering – that are attuned to the social organization of their activity, in which security requirements are just one small part of a wide landscape of social norms of trust and coordination that orient action.

We start from this classification of users' models in security scientific literature and we highlight shared assumptions that can orient research. We then examine the empirical diversity of user profiles in the European Union (EU 27, without including Croatia that became a member in 2013), using the Eurobarometer 77.2/2012 cross-sectional dataset (European Commission, 2012a). The article is structured as follows: the next section discusses theoretical implications of current research on end-users' security practices, focusing on the interdependence between risk awareness and response, experiences of personal loss due to cyber-crime, and users' activity. We then formulate research questions and we discuss the methodology of survey-based research and our specific choice of methods. We present research results, comparing linear causal modeling of behavior with classification analysis. We then conclude the paper, discuss its strengths and limitations, and we propose fruitful avenues for further survey research.

Theoretical perspectives: models of end-users in security research

Users may be analyzed through various theoretical perspectives. We discuss below three models that orient investigations by directing attention to different aspects deemed relevant for users' actions: the 'lazy user', the 'economically rational user', and the 'social user'. These models are ideal types useful for analytical purposes, rather than empirical categories; a person's behavior may be interpreted in relation to each theoretical perspective. Authors usually privilege one model over the others, but also include considerations from elsewhere. All three models accommodate risk-averse and risk-seeking behaviors, but propose different constraints on users' activity: avoidance of cognitive overloading, preference for economic optimization, and pursuit of social integration, respectively.

A core issue for describing end-users' security behaviors refers to *risk awareness* (see a succinct comparison in Table 1). From the perspective of the *lazy user*, awareness is mainly a function of users' understanding of online technologies and risks and, reciprocally, the accessibility of security solutions (Adams and Sasse, 1999; Albrechtsen and Hovden, 2009; Besnard and Arief, 2004; Furnell et al., 2007; Furnell et al., 2006). 'Lazy' end-users are usually portrayed as technically naïve. At the same time, users are vulnerable because they must allocate scarce cognitive resources to multiple, competing tasks. Attending to security issues enters in conflict with attending to other tasks that are also cognitively demanding, and users need to balance multiple goals: 'humans obey least-effort rules because they are cognitive machines that attempt to cheaply reach flexible objectives rather than to act perfectly towards fixed targets' (Besnard and Arief, 2004).

From the perspective of the *economically rational user* (Christin et al., 2012; Herley, 2009), awareness is primarily a function of experienced personal loss due to cybercrime, as well as of general information of losses experienced by similar others. Loss is dependent on activity: different types of online activities may incur different types of losses; also, the frequency of online exposure increases the frequency of actual losses that materialize the risk. An important observation here is that losses are distributed among different participants to a cybercrime setting, through various social arrangements. For example, in the case of hacked banking accounts, losses are distributed between the bank and the end users – and, consequently, end users are often protected from cybercrime risks by arrangements that transfer financial losses to corporate actors. Losses may also be hidden, appearing more like a minor inconvenience. Moreover, security measures have non-negligible costs (Herley, 2009; Inglesant and Sasse, 2010). Users are portrayed as economically rational actors who estimate risks and protection costs based on their own experiences and those of relevant others, and adjust their protective behavior to efficiently pursue their activity, as they understand it.

From the perspective of the *social user* (Weirich and Sasse, 2001), awareness is created through personal experiences, of self and others, that are socially interpreted through shared 'folk

Table 1 – Three theoretical models of end-users as security actors.

	Cognitively lazy users	Economically rational users	Social users
Portrayal focus	Technical naïveté, due to multiple objectives	Economic rationality in the context of one's own activity	Self-presentation concerns; trustful actors, in pursuit of concerted activities
Users' risk awareness	Awareness is dim, risks are underestimated	Awareness is adequate, reflecting estimated personal risks	Relevant risks are socially defined, through communication that gives meaning to personal experiences
Rationality	Bounded, based on heuristics	Economical, based on cost-benefit analysis	Rationality appears as a byproduct of activities of justification (accounting), using socially constructed vocabularies
Main springs of action	Satisficing on goals Minimizing effort	Optimizing the pursuit of preferences	Achieving legitimate goals and maintaining desired identities in the local social order
Reasons for low compliance	Low understanding of risks and low technical expertise	Average end-user losses from cybercrime are perceived to be low; Security costs are high; Future costs and benefits are discounted	Security practices are: - Obstacles for smooth social organization - Associated with de-valued identities