Chapter 48
Cyberloafing in the Workplace

Christine A. Henle
Colorado State University, USA

Uma Kedharnath
Colorado State University, USA

ABSTRACT
Cyberloafing is employees’ intentional use of Internet technology during work hours for personal purposes. This can include surfing non-work related Internet sites, sending personal emails, online gaming, or social networking. Given the prevalence of cyberloafing and its negative consequences (e.g., reduced productivity, network clogging, security breaches), organizations have responded by implementing Internet use policies, filtering or monitoring Internet activity, and disciplining policy violators. Recently, attention has shifted away from identifying methods to limit cyberloafing to pinpointing the causes of cyberloafing. This emerging research suggests that employees are more likely to cyberloaf when they are treated unfairly, have certain characteristics like external locus of control or higher work status, have positive attitudes toward cyberloafing, or there are norms supporting it. The authors offer directions for future research that include exploring the possibility that cyberloafing can lead to positive outcomes like increased job performance, reduced stress, and work-life balance.

INTRODUCTION
The Internet offers businesses a fast and efficient way to gather information, generate ideas, communicate, and conduct business. Although the Internet enables companies to operate anywhere, anytime, there is a dark side to this technology in the workplace. Unfortunately, it also offers a convenient way for employees to avoid or shirk their work duties and responsibilities. Employees have long found ways to do this in the form of gathering around the “water cooler”, making personal phone calls, or taking frequent smoking, restroom, or lunch breaks. However, unlike its predecessors, the Internet allows employees to maintain the appearance of being hard at work.
since they do not have to leave their desks and
can quickly minimize Internet browsers or put
away their smartphones.

Cyberloafing refers to employees’ intentional
use of Internet technology during work hours for
personal purposes. This technology can be com-
pany provided or personal devices that employees
bring with them to work (e.g., smartphone, iPad).
Cyberloafing is a form of production deviance,
which means that it violates organizational norms
regarding minimal levels of quantity and quality
of production. As such, it involves employees
wasting time at work instead of completing their
required job duties at an acceptable standard of
performance. Cyberloafing has also been referred
to as cyberslacking, Internet abuse, non-work-
related computing, personal web usage, workplace
Internet deviance, and cyber-production deviance.
However, we do not include Internet addiction
in our definition as this denotes excessive and
compulsive use of the Internet in both work and
non-work settings and only impacts a very small
proportion of Internet users.

Organizations are cognizant of cyberloafing
because of the negative impact it can have. First,
it can detract from productivity since employees
are concentrating on non-work related activities
instead of performing their jobs. This hurts com-
panies’ bottom-line in the form of lost wages as
well as reduced output and profitability. Second,
cyberloafing takes a toll on computing resources
within companies. Employees’ personal use of
company provided Internet access can tax the
computing system, which in turn reduces band-
width and degrades system performance. Next,
cyberloafing puts companies at risk for security
breaches, viruses, and hacking as well as legal li-
ability in the form of harassment (e.g., an employee
emailing racist or sexist jokes to coworkers),
defamation (e.g., a disgruntled manager posting
lies about a former employee on Facebook), and
negligent hiring (e.g., an employee with a history
of violence cyberstalking a customer). These det-
rimental effects have led researchers to investigate
cyberloafing in an effort to deter it.

HISTORICAL BACKGROUND

Traditionally, research on cyberloafing has been
descriptive (Lim, 2002). These studies have ex-
amined the frequency that employees cyberloaf
and the particular types of Internet sites they
visit. Once the prevalence of cyberloafing was
documented, attention then turned to developing
reactive solutions to it. This body of work focused
on identifying ways that organizations can prevent
or minimize cyberloafing and included things
like implementing Internet use policies, using
filtering or monitoring software, and disciplining
those caught cyberloafing. Below we describe the
historical development of a typology of cyberloaf-
ing as well as the generation of deterrent methods
for cyberloafing.

Typology of Cyberloafing

Establishing a typology of cyberloafing was an im-
portant first step in the literature because different
types of cyberloafing may have unique anteced-
ents and consequences, thus requiring distinctive
remedies. Lim (2002) originally differentiated
cyberloafing into browsing and email activities.
The former includes surfing non-work related
Internet sites pertaining to social networking,
news, banking, sports, shopping, entertainment,
pornography, and so forth while the latter entails
checking, receiving and sending personal email.
Lim found support for this two-factor structure
using a sample of employed adults in Singapore.
However, she collapsed the two dimensions when
she empirically explored cyberloafing so we do
not know whether the types of cyberloafing have
differential predictors or outcomes.