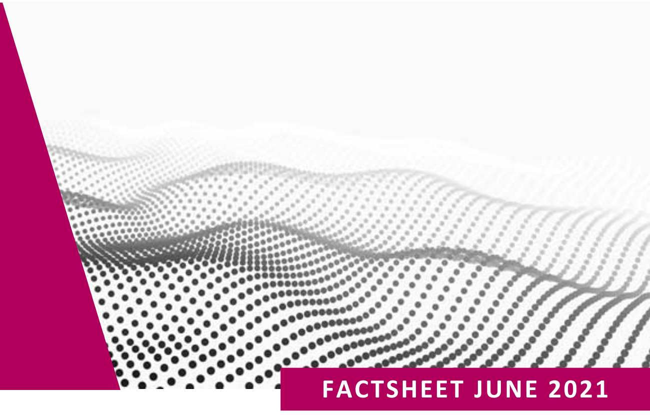
nscr
Nederlands Studiecentrum
Criminaliteit en Rechtshandhaving

What Works in **Situational Cybercrime Prevention?**



FACTSHEET JUNE 2021

For decades, situational crime prevention techniques have consistently proven effective in reducing various forms of crime in a range of contexts. In many cases, their success has been supported by experimental evidence, earning this preventive paradigm worldwide recognition. Inspired by this story of success, cybercrime researchers have sought to extend their application to cyberspace.

Despite the wide variety of techniques offered by situational crime prevention, criminologists have applied just a few to tackle cybercrime. For example, researchers have evaluated the effectiveness of antivirus software in detecting malware; the ability of monitoring software to detect anomalous patterns of activity among employees; and—especially—the effect of warning banners on cybercriminal behavior.

Situational crime prevention

Situational crime prevention consists of the implementation of a set of 25 techniques to reduce specific forms of crime through five mechanisms: (1) increasing the effort required to commit a crime, (2) increase the risk of detection, (3) reduce the potential rewards of crime, (4) reduce provocations to potential offenders, and (5) eliminate excuses for non-compliance. These techniques work immediately before the crime occurs when all previous crime controls, such as personal and social, have failed. And if situational crime prevention fails, only formal crime controls, such as the police or the criminal justice system, can be invoked. Formal sanctions are not only costly but sometimes involve measures that conflict with people's rights—so it is best to avoid them if possible.

This overview of what works in situational cybercrime prevention focuses on research that has high validity. We only examine studies that measure cybercrime before and after an intervention in experimental and comparable control conditions; this is, studies that scored three or more in the Maryland Scientific Methods Scale. The only studies that meet this criterion are experiments with warning banners.

Experiments with online warning banners

Online warning banners are small text frames that are usually displayed to users when they try to access a system or a website. They work in the same way as a traditional sign: they are placed in easily visible places to persuade the reader with a clear short message. Criminologists have used such banners to increase the perceived risk by cyber offenders or to remove any excuse they might have for non-compliance. But how is this done in cyberspace?

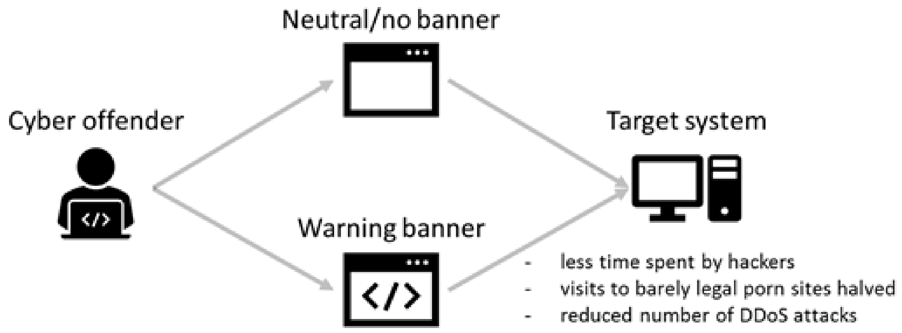
To measure the effect of banners on human behavior, researchers use experiments with honeypots: digital decoys designed to be attacked that collect data on the attack and the behavior of the offenders. Once cyber offenders fall into the trap, they are randomly assigned in groups to different stimuli—a banner with a text. Banners can contain, for example, deterring messages such as “you are being watched” or “this is illegal”, or neutral ones such as “the site is loading”. In some cases, one of the groups may not receive any message at all. This strategy allows to compare the effect of different stimuli on similar groups of offenders to identify which one works best.

So ... do banners work?

Experiments with warning banners have mainly been aimed at deterring hackers from trespassing into systems. However, banners have also been used recently to deter users from consuming barely legal pornography and from carrying out Distributed Denial of Service (DDoS) attacks.

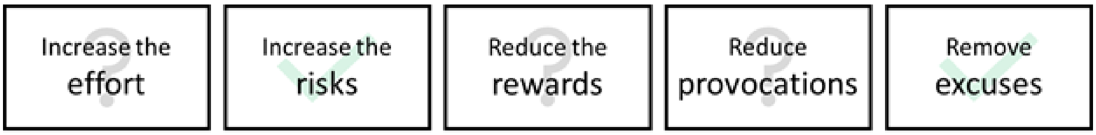
For hacking, experiments measured the effect of banners on four types of behavior: number of trespassing events, number of repeated trespassing events, duration of the trespassing, and volume of commands entered into the system. The results show a mixed effect in reducing the number of trespassing and repeated trespassing events, as well as the number of commands entered by the attacker into the system. In other words, while some banners reduced some of these behaviors, others had no effect. However, the banners appear to significantly reduce the duration of the trespassing; this is, the time spent by the offender inside the system.

As for the single experiment on pornography, banners displaying a deterrent message halved the volume of accesses to the website hosting the barely legal content. And when banners were used to divert young people from carrying out DDoS attacks, researchers observed a change in the increasing trend of attacks to a flat trend. Overall, the effect of banners is mixed, but promising in some areas.


Neutral/no banner
Cyber offender
Target system
Warning banner
- less time spent by hackers
- visits to barely legal porn sites halved
- reduced number of DDoS attacks

Conclusion

Despite the growing interest in tackling cybercrime, experimental research on the effect of situational crime prevention techniques on deflecting cyber offenders is still in its infancy. High validity research has only evaluated the effect of a few techniques. With a few exceptions, criminologists have focused on increasing the perceived risk of being detected and removing excuses for non-compliance through the use of warning banners—especially—to deter hackers from breaking into a system. While it is not yet clear whether banners are always an effective tool for reducing cybercrime, experiments show promising results in specific contexts. To strengthen the evidence base, more research is needed not only on the effect of banners, but also on the effect of other situational crime prevention techniques that remain unexamined.



Situational crime prevention categories frequently examined with warning banners

Contact: Asier Moneva | AMoneva@nscr.nl & Jim Schiks | JSchiks@nscr.nl

Further reading

- Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). Cybercrime Prevention: Theory and Applications. Springer International Publishing. https://doi.org/10.1007/978-3-030-31069-1
- Clarke, R. V. (2017). Situational crime prevention. In R. Wortley & M. Townsley (Eds.), Environmental Criminology and Crime Analysis (2nd ed., pp. 1–25). Routledge, Taylor & Francis Group.
- Collier, B., Thomas, D. R., Clayton, R., & Hutchings, A. (2019). Booting the Booters: Evaluating the Effects of Police Interventions in the Market for Denial-of-Service Attacks. Proceedings of the Internet Measurement Conference, 50–64. https://doi.org/10.1145/3355369.3355592
- Farrington, D. P., Gottfredson, D. C., Sherman, L. W., & Welsh, B. C. (2003). The Maryland Scientific Methods Scale. In D. P. Farrington, D. L. MacKenzie, L. W. Sherman, & B. C. Welsh (Eds.), Evidence-Based Crime Prevention (pp. 13–21). Routledge. https://doi.org/10.4324/9780203166697
- Leukfeldt, E. R., & Jansen, J. (2020). Financial cybercrimes and situational crime prevention. In E. R. Leukfeldt & T. J. Holt (Eds.), The Human Factor of Cybercrime (pp. 216–239). Routledge.
- Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014). Restrictive deterrent effects of a warning banner in an attacked computer system. Criminology, 52(1), 33–59. https://doi.org/10.1111/1745-9125.12028