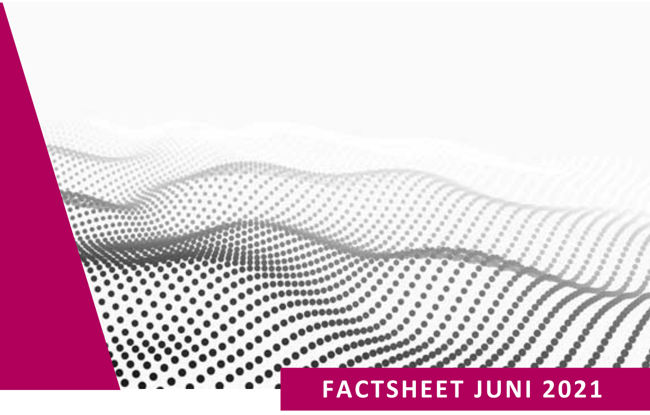
nscr
Nederlands Studiecentrum
Criminaliteit en Rechtshandhaving

What Works?
Situationele Cybercrimepreventie



FACTSHEET JUNI 2021

Al tientallen jaren blijken technieken voor situationele criminaliteitspreventie effectief in het tegengaan van verschillende vormen van criminaliteit. Vaak wordt dit ondersteund door experimenteel bewijs, waardoor dit preventieve paradigma wereldwijde erkenning heeft gekregen. Geïnspireerd door dit succesverhaal hebben onderzoekers op het gebied van cybercrime geprobeerd de toepassing uit te breiden naar de digitale wereld.

Ondanks de grote verscheidenheid aan technieken die situationele criminaliteitspreventie te bieden heeft, hebben criminologen pas enkele daarvan toegepast bij de aanpak van cybercrime. Zo zijn er evaluaties uitgevoerd naar de effectiviteit van antivirussoftware bij het detecteren van malware, naar het vermogen van monitoringssoftware om afwijkende activiteitspatronen bij werknemers te detecteren, en vooral naar het effect van waarschuwingsbanners op het gedrag van cybercriminelen.

Situationele criminaliteitspreventie

Situationele criminaliteitspreventie bestaat uit de implementatie van een reeks van 25 technieken om specifieke vormen van criminaliteit te verminderen, door middel van vijf mechanismen: (1) het verhogen van de inspanning die nodig is om een delict te plegen, (2) het verhogen van het risico om gepakt te worden, (3) het verminderen van de potentiële beloningen van criminaliteit, (4) het verminderen van provocaties richting potentiële daders en (5) het wegnemen van excuses voor crimineel gedrag. Deze technieken werken vóór dat de misdaad plaatsvindt, wanneer eerdere interventies op bijvoorbeeld persoonlijk of sociaal niveau niet hebben gewerkt. Wanneer ook technieken voor situationele criminaliteitspreventie niet werken, kunnen alleen formele criminaliteitsinterventies zoals de politie en het strafrechtelijk systeem worden ingeschakeld. Deze formele sancties zijn niet alleen kostbaar, maar omvatten soms ook maatregelen die in strijd zijn met de rechten van de mens.

Dit overzicht van wat werkt bij de situationele preventie van cybercrime is gericht op studies met een hoge validiteit. Alleen studies die cybercrime voor en na een interventie meten in experimentele en vergelijkbare omstandigheden zijn gebruikt. Dit zijn studies die een score van drie of hoger hadden op de Maryland Scientific Methods Scale. De enige onderzoeken die aan dit criterium voldoen zijn experimenten met waarschuwingsbanners.

Experimenten met waarschuwingsbanners

Online waarschuwingsbanners zijn kleine tekstkaders die normaal gesproken worden getoond wanneer gebruikers toegang proberen te krijgen tot een systeem of website. Ze werken op dezelfde manier als een traditioneel bord: ze worden goed zichtbaar geplaatst om de lezer te overtuigen met een korte, duidelijke boodschap. Criminologen hebben dergelijke banners gebruikt om het door cybercriminelen waargenomen risico te verhogen of om de excuses die zij mogelijk hebben voor crimineel gedrag weg te nemen. Maar hoe werkt dit in de digitale wereld?

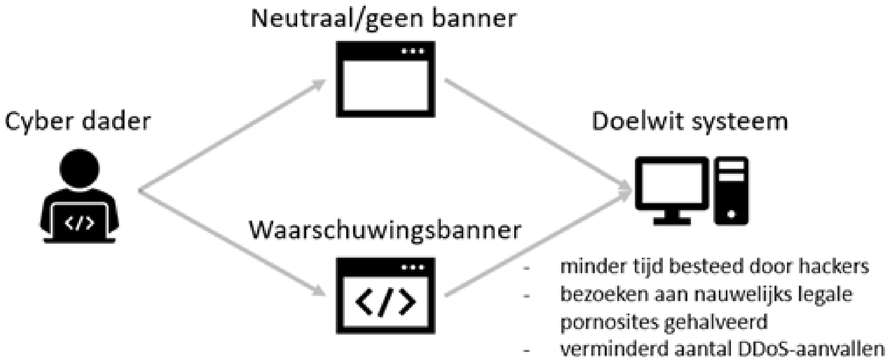
Om het effect van banners op menselijk gedrag te meten, gebruiken onderzoekers experimenten met zogenaamde *honeypots:* digitaal lokaas, ontworpen om aangevallen te worden en gegevens te verzamelen over de aanval en het gedrag van de daders. Eenmaal in de val gelopen, worden de cybercriminelen willekeurig aan groepen toegewezen met verschillende prikkels: een banner met een tekst. Banners kunnen bijvoorbeeld afschrikkende berichten bevatten, zoals ‘je wordt in de gaten gehouden’ of ‘dit is illegaal’, of neutrale berichten zoals ‘de site wordt geladen’. In sommige gevallen ontvangt een groep helemaal geen bericht. Een dergelijke strategie maakt het mogelijk om het effect van verschillende prikkels op vergelijkbare groepen daders tegen elkaar af te zetten, en zo te bepalen welke prikkel het beste werkt.

Dus ... werken banners?

Experimenten met waarschuwingsbanners zijn er vooral op gericht om hackers af te schrikken bij het binnendringen van systemen. Ook worden banners gebruikt om bezoekers ervan te weerhouden nauwelijks legale pornografie te bekijken en om DDoS-aanvallen (Distributed Denial of Service) uit te voeren.

In experimenten is het effect van banners bij hacken gemeten voor vier soorten gedrag: het aantal overtredingen, het aantal herhaalde overtredingen, de duur van de overtreding en het aantal commando's dat in het system is ingevoerd. De resultaten laten een gemengd effect zien bij het verminderen van het aantal overtredingen en herhaalde overtredingen, evenals het aantal commando's dat door de aanvaller in het systeem wordt ingevoerd. Met andere woorden: terwijl sommige banners sommige van deze gedragingen verminderden, hadden andere geen effect. De banners blijken echter de duur van de overtreding – de tijd die de dader in het systeem doorbrengt - aanzienlijk te verkorten.

Binnen het experiment met pornografie halveerden de banners met een afschrikkende boodschap het aantal keren dat er toegang werd verschaft tot de website. Wanneer banners werden gebruikt om jongeren ervan te weerhouden DDoS-aanvallen uit te voeren, zagen onderzoekers een verandering van een toenemende trend van aanvallen naar een gelijkblijvende trend. Over het algemeen is het effect van banners gemengd, en op sommige gebieden veelbelovend.



- minder tijd besteed door hackers
- bezoeken aan nauwelijks legale pornosites gehalveerd
- verminderd aantal DDoS-aanvallen

Conclusie

Ondanks de toenemende belangstelling voor de aanpak van cybercrime, staat experimenteel onderzoek naar het effect van situationele criminaliteitspreventie gericht op cybercriminelen nog in de kinderschoenen. Onderzoek met een hoge validiteit heeft slechts van enkele technieken het effect onderzocht. Criminologen hebben zich hoofdzakelijk gericht op het verhogen van het waargenomen risico om ontdekt te worden en het wegnemen van excuses voor crimineel gedrag, door het gebruik van waarschuwingsbanners om hackers ervan te weerhouden in te breken in een systeem. Hoewel het nog niet duidelijk is of banners altijd een effectief middel zijn om cybercrime terug te dringen, laten experimenten in specifieke contexten veelbelovende resultaten zien. Om de wetenschappelijke basis te versterken, is meer onderzoek nodig. Niet alleen naar het effect van banners, maar ook naar het effect van andere situationele criminaliteitspreventietechnieken die nog niet zijn onderzocht.

Situationele criminaliteitspreventie technieken vaak onderzocht met waarschuwingsbanners

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

Verder lezen

- 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