Conclusions The results thus shed more light on the extent to which criminological theories are applicable across different types of Internet-related crime.

Een onderzoek naar de redenen van effectiviteit van phishing emails

L. Mol, E.E.H. Lastdrager, M. Junger, J.M. Heerkens

Achtergrond Phishing is het zich via internet opzettelijk anders voorstellen met als doel andere mensen te duperen en daaruit zelf winst te halen. Door globalisering en digitalisering van vele diensten (denk bijvoorbeeld aan internetbankieren) vormt dit een steeds groter maatschappelijk probleem.

Doel Het onderzoek stelt zich ten doel uit te vinden welke criteria personen in overweging nemen om te bepalen of een mail al dan niet betrouwbaar is en waarom zij er al dan niet op ingaan. Om zodoende meer inzicht te krijgen in de beweegredenen van individuen bij het lezen en reageren op (phishing)mails.

Methode Dit onderzoek zal uitgevoerd worden door middel van een think aloud experiment, waarbij 15 personen in experimentele setting een mail zullen doornemen en daarna geïnterviewd worden. Analyse van de data wordt gedaan aan de hand van de literatuur over bedrog van Cialdini en andere criteria voortkomend uit de literatuur, om zodoende te bepalen welke criteria ook écht een grote rol spelen bij het vallen voor phishingmails. De deelnemers aan het experiment zullen vooraf niet weten dat het hier om phishing gaat.

Resultaten

Conclusies

Modus Operandi Study of Information and Communication Technology (ICT) Facilitated Crime

Lorena Montoya, Marianne Junger, Pieter Hartel

Background How can one measure the prevalence of cybercrime? One option is to define cybercrime as a specific form of crime, and then quantify it using, for example, police files. Domenie, Leukfeldt, Toutenhoofd-Visser, and Stol (2009) used this approach and concluded that between 0.42% and 0.66% of all crime reported to the police constitutes cybercrime. An alternative is to keep traditional definitions of crime and quantify the amount of associated ICT.

Aim The present research established how ‘digital’ crimes currently classified as ‘traditional crimes’ are.

Methodes We collected information on residential and commercial burglary, threats and fraud. 809 incidents from the Police Department of East Netherlands were studied. The data collected consisted of information on incidents, victims and suspect characteristics. We determined how much ICT was used a)in 3 phases of the 'crime script' (i.e. before, during and after), b)during the criminal investigation and c) in the apprehension of the suspect (s).

Results In total, 136 burglaries, 140 commercial burglaries, 259 threats and 274 cases of fraud were studied. The results show that ICT is used in 16% of the threats; and 41% of the fraud cases. Among residential burglaries, 3% of the cases involved IT, mostly after the offense. IT is not used in commercial burglaries. We will discuss the characteristics of offenders and victims of digital crimes.

Conclusion The main conclusion is that ICT plays a greater role in traditional crime than first expected. The implications of the findings for the measurement of cybercrime will be discussed.

Diefstal van 'verloren' USB sticks

Elmer Lastdrager, Denise Foppen, Lorena Montoya, Pieter Hartel, Marianne Junger

Achtergrond Dataverlies is een groot probleem binnen organisaties. Er zijn legio voorbeelden van verloren usb sticks in de trein, waarna gevoelige data op straat kwam te liggen. Versleuteling is een oplossing om de vertrouwelijkheid van de data te waarborgen, maar biedt uiteraard geen bescherming tegen verlies.

Doel Het doel van deze studie is inzichtelijk te maken hoe vaak verloren usb sticks worden gestolen. Ook willen we weten of er verschillen zijn tussen mensen die de usb sticks inleveren bij een receptie en de mensen die de usb sticks stelen. Daarnaast zijn testen we of het markeren van usb sticks met labels, bijvoorbeeld met informatie over de eigenaar of een indicatie van de inhoud, invloed heeft op het al dan niet terugbrengen.

Methode Wij introduceren een variant van het lost-letter experiment (Merritt & Fowler 1948; Milgram, Leon & Harter 1965) waarbij usb sticks neergelegd worden binnen de gebouwen van enkele onderwijsinstellingen. Na het neerleggen wordt de usb stick geobserveerd en zodra iemand hem oppakt worden zowel de situatie als kenmerken van de betreffende persoon vastgelegd.