



Så kan beteendeanalys motverka bedrägerier

Gareth Williams



S
VONNA

BANK

SAAB

10

733

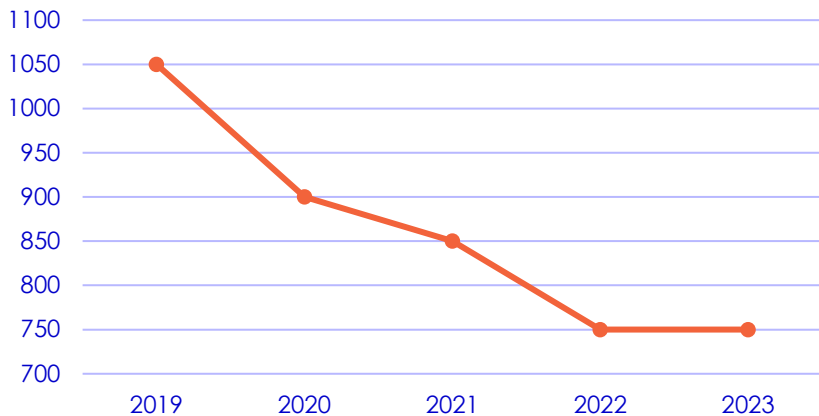
OLIVIERO
TOSCANI



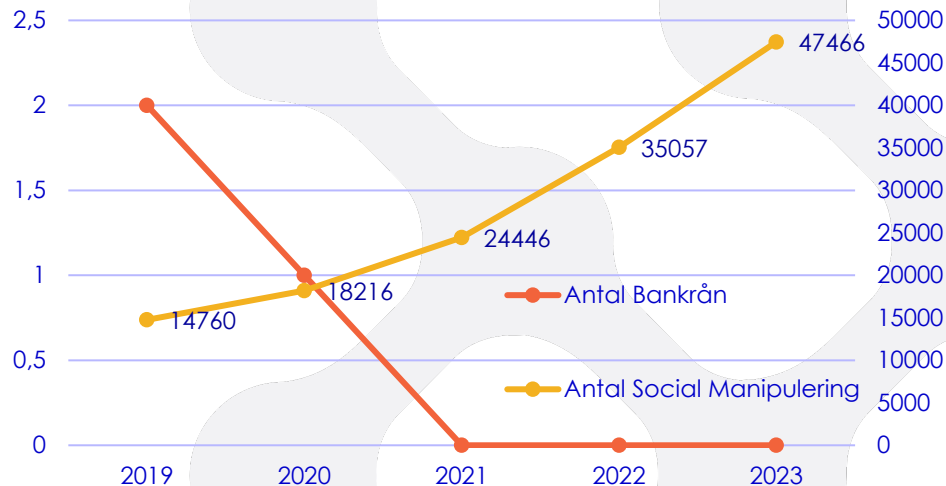
Världen har ändrats. Kriminaliteten också

År 1985: 1320 Bankkontor i landet

Antal Bankkontor i Sverige



År 1985: 106 Bankrån i landet



Källa: Sveriges Riksbank, BRÅ

UPPDRAG
GRANSKNING

“Vi säljer rädsla”

FÖLJ LIGAN FRÅN INSIDAN

BEDRAGARNA

Att tolka känslor var lite enklare på 80-talet



Engagerad



Förvirrad



Tveksam



Frustrerad



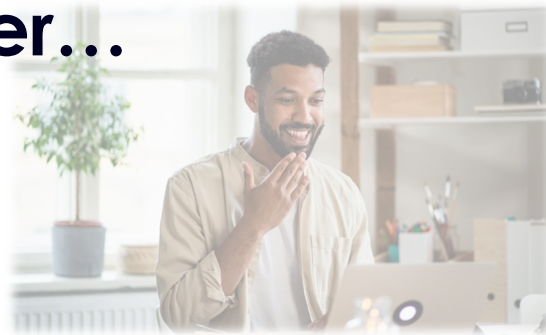
Distraherad



Beteendeanalys

“Digitalt kroppsspråk”

Hur man bygger beteendeinsikter...



Behavioral Insights

- Data familiarity
- Hesitation
- Distraction
- Process familiarity
- Duress
- Being guided
- User expertise
- Age analysis

Behavioral Biometrics: User Profiling

- Swiping
- Holding
- Interaction preferences
- Tremors
- Press size
- Hand-eye co-ordination
- Typing cadence
- Navigation patterns

Cognitive Analysis: Patterns

- Use of shortcuts
- Long term memory
- Abnormal interactions
- Copy and paste
- Selection
- Decision making
- Segmented typing
- Aimless Mouse movement

Collect Data



Keystroke
movement



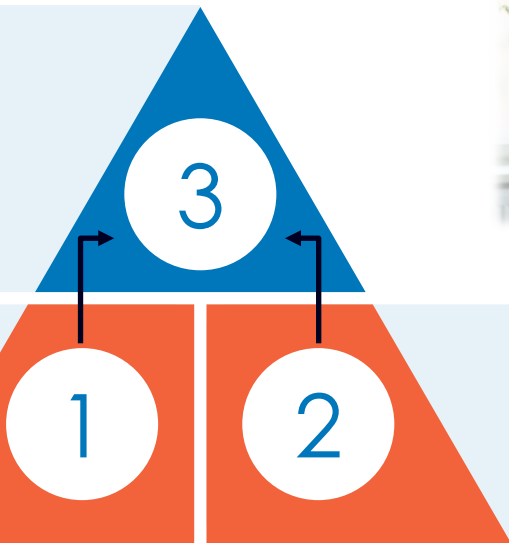
Mouse
activity



Touch screen
behavior



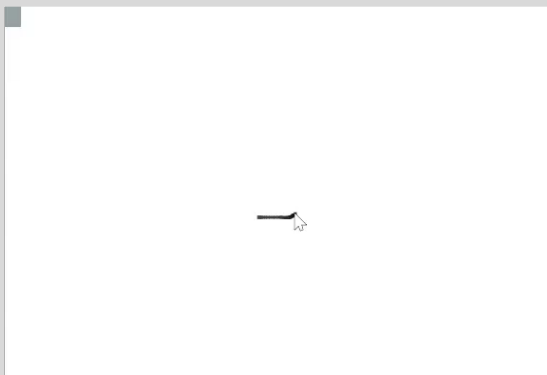
Mobile
device
movement



...För att upptäcka telefonbedrägerier

1

På datorn: Verkar de distraherade?



Mållösa musrörelser eller "musklotter" är en indikation på att en användare är distraherad och håller sessionen aktiv

2

På datorn: Tvekar de?

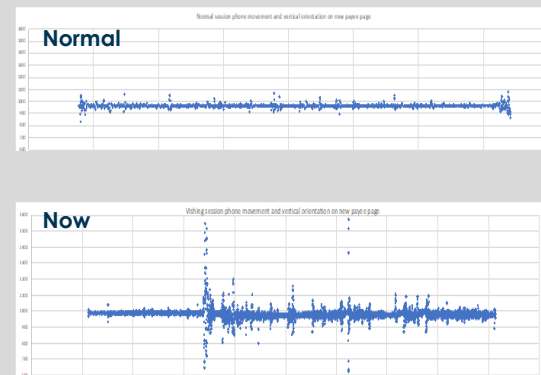
Duration of mouse click on payment submit button



Längre musklick är subtila indikationer på tvekan över att göra betalningen

3

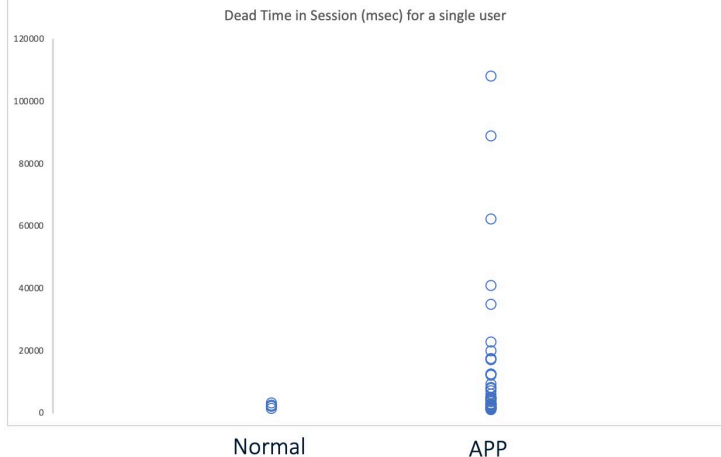
På mobilen: Får de vägledning?



Telefonrörelser kan tyda på att en användare flyttar telefonen till och från örat, vilket indikerar att de är i ett samtal. I mobilen kan vi också upptäcka om användaren är i ett aktivt telefonsamtal.

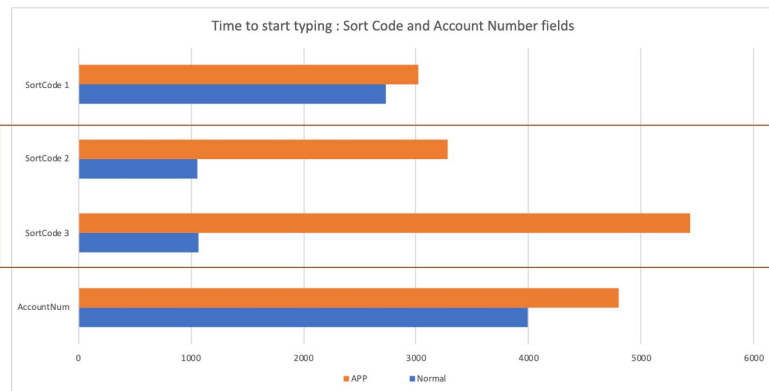
Beteendemässiga egenskaper vid telefonbedrägerier

DISTRAKTION



En normal session för offret visar nästan ingen "dödtid". Användaren är målmedveten med sin navigering. I telefonbedrägerisessionen finns det många och ofta långa perioder av "dödtid". Detta indikerar att användaren är distraherad.

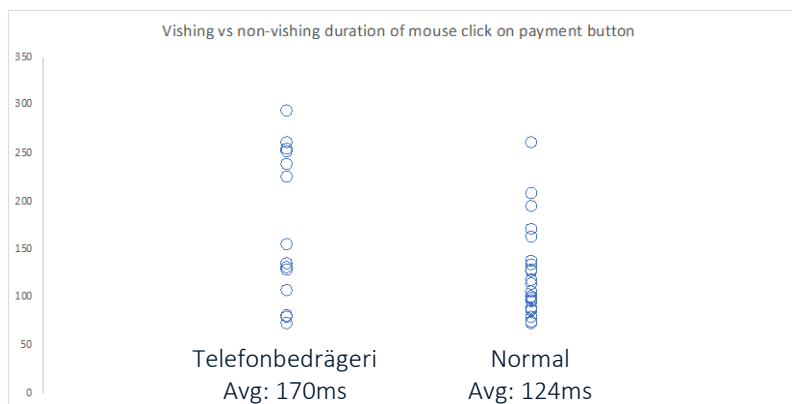
DIKTAMEN



De första 2 clearingnummersiffrorna för både den genuina och den bedrägliga transaktionen tar lika lång tid för användaren att skriva eftersom de hänvisar till sin referenspunkt. Vi ser dock att i fälten för 2:a och 3:e clearingsiffran börjar användaren skriva mycket snabbare i den normala sessionen än i telefonbedrägerisessionen. I telefonbedrägerisessioner väntar användaren på instruktioner och upprepar siffrorna som mottagits tillbaka till bedrägaren

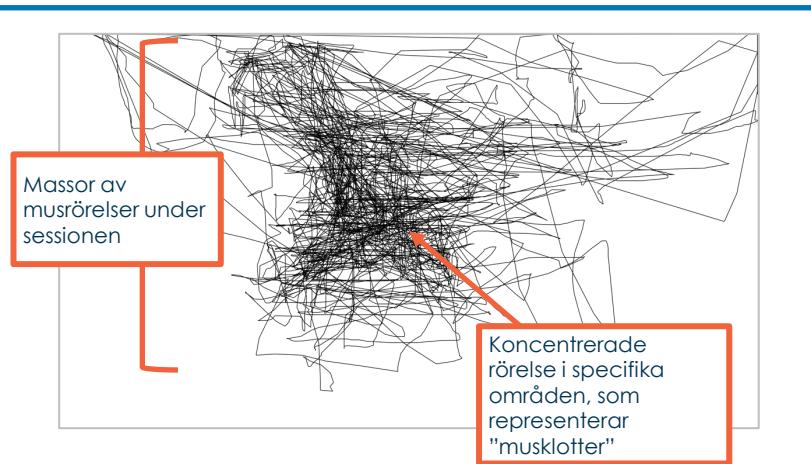
Beteendemässiga egenskaper vid telefonbedrägerier

TVEKAN



I normala sessioner ser vi att den genomsnittliga varaktigheten av musklicket på knappen för att skicka betalning är 124ms. I telefonbedrägerisessioner är genomsnittet 170ms. En längre varaktighet vid klick på betalning indikerar att användaren tvekar och tillfälligt pausar för att ifrågasätta om de ska göra betalningen.

MÅLLÖSA RÖRELSE

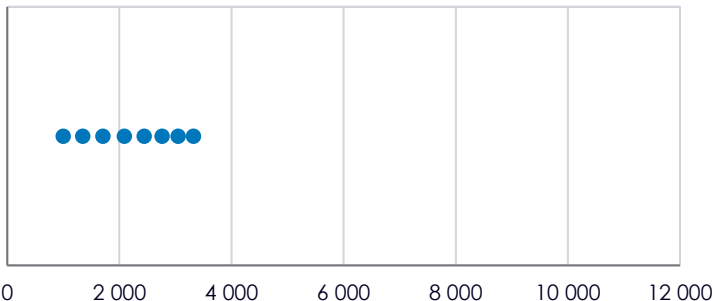


Musklotter och mållösa musrörelser är en tydlig indikation på att användaren är distraherad och håller sessionen aktiv medan de blir socialt manipulerade av bedragaren. Telefonbedrägerisessioner har vanligtvis mycket mer musaktivitet än vad som ses i vanliga sessioner i koncentrerade fickor.

Beteendemässiga egenskaper vid telefonbedrägerier

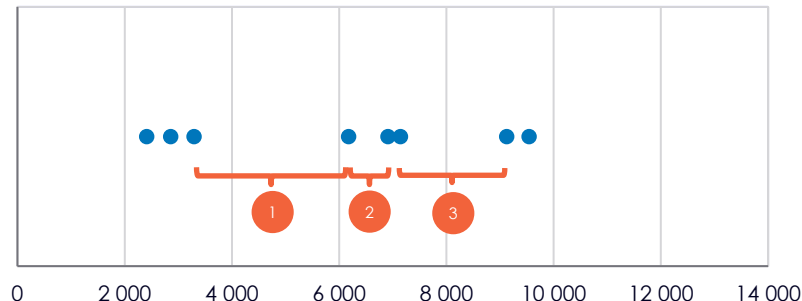
Nya betalningsmottagare

INMATNING AV ÄKTA KONTONUMMER



- Uppgifter om betalningsmottagarens namn och kontonummer matas in från användarens minne - flytande inmatning
- Ingen indikation på diktering
- Inga felkorrigeringar
- Snabb inmatning
- De längsta 3 pauserna i den genuina sessionen är ungefär hälften av de för telefonbedrägerisessionerna

INMATNING AV KONTONUMMER UNDER TELEFONBEDRÄGERI



3 längsta pauser

- 1 2,884 ms
- 2 731 ms
- 3 1982 ms

- 9,5 sekunder för att ange kontonummer
- 2,5 sekunders fördröjning för att börja skriva
- Inmatningsbeteendet skiljer sig från en genuin session
- Dikteras i två grupper om 3 siffror och sedan 2 siffror i slutet
- Skrivmönster och pauser indikerar att kontonumret dikteras

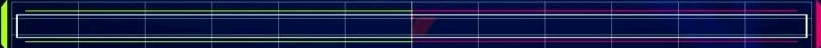
Victim

00:00:01

BioCatch



Low Risk



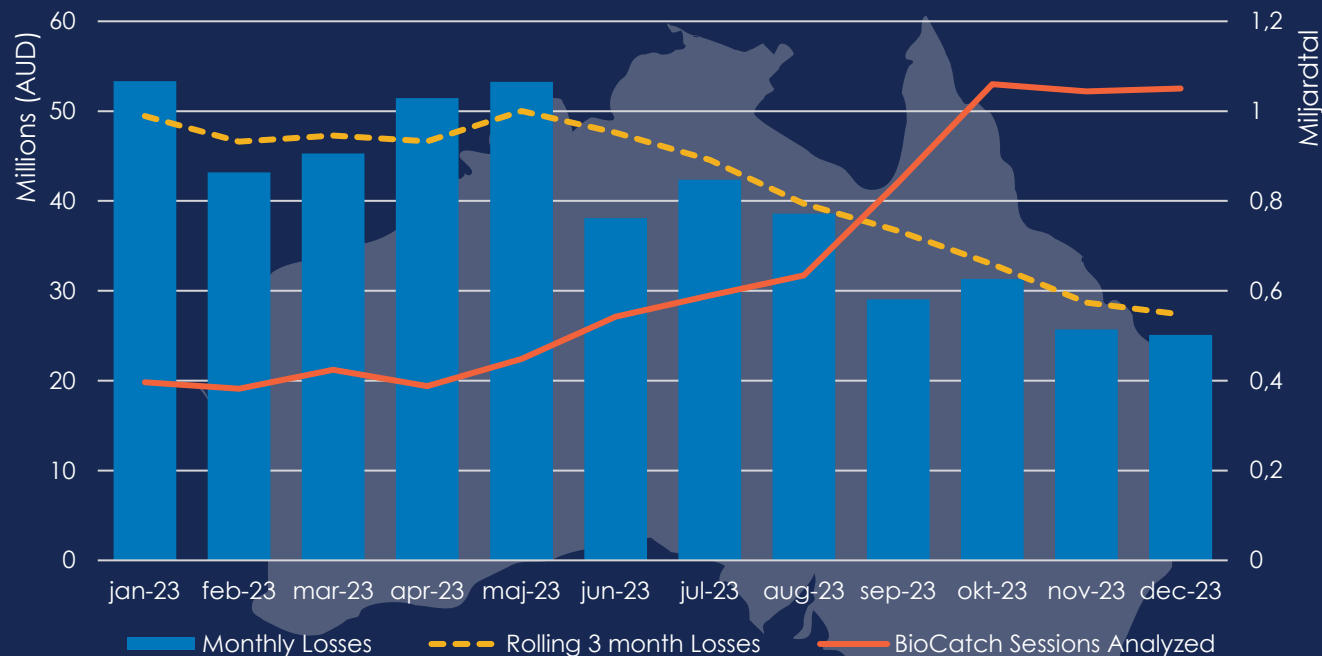
High Risk



Ett globalt problem?

Vissa länder håller på att motverka trenden

Australien ligger i framkant



**53 %
minskning
av
förlusterna
under
2023**

Datakälla: scamwatch.gov.au

Beteendeeinformation berättar om känslor



Engagerad

- Snabb skrivhastighet
- Snabba svar på sidändringar
- Snabba, direkta och smidiga musrörelser



Förvirrad

- Ökade varv med musen
- Avståndet mellan klick är större än genomsnittet
- Musbesök och flera klick på samma plats



Tveksam

- Pauser före klick
- Mindre musslag
- Långsam hastighet/acceleration i musrörelser



Frustrerad

- Snabba, sporadiska musrörelser
- Överdrivet klickande med ökat tryck
- Skrivfel



Distraherad

- Klottra med musen
- Inaktivitet (musen är inaktiv, ingen interaktion med tangentbordet)
- Markering av Innehåll

Vi vet att bedragare har lyckats spela på kundernas känslor – Det är dags att slå tillbaka!



BANK
BANK

VOLVO

SWEVO SAB

SVEVIGEN



REKREATION
SVEVIGEN
SVEVIGEN

2017/1001

2017/1001

Lär dig mer om
BioCatch:



BioCatch

(det här är inte quishing!)

Gareth på LinkedIn:

