«Alt som glitrer er gull»
Hvordan unngå kyniske bedragere

Terje Aleksander Fjeldvær
Head of Sanctions & Fraud Prevention

Tapper norske bedrifter for hundrevis av millioner: Slik opererer de nye digitale ranerne

Stortinget utsatt for et omfattende IT-angrep

STORTINGET (NRK): Stortinget har blitt utsatt for et omfattende IT-angrep. Det er registrert innbrudd på e-post-kontoene hos et mindre antall stortingsrepresentanter og ansatte. Saken er anmeldt til PST.

SE VIDEO: Pressemøtet på Stortinget om IT-angrepet.

Cyberangrep koster opptil 450 millioner

Svindelforsøk mot 26.000 DNB-kort – storbanken har sperret flere kort

Massivt data-angrep mot flere av Norges største bedrifter

Visma utsatt for hackerangrep fra Kina

Mistenker at en fremmed stat står bak hackerangrep

Profesjonelle hackere brøt seg inn i datasystemene til helseforetaket Helse Sør-Øst i forrige uke. Nå mistenker PST mulig etterretningsvirksomhet fra en fremmed stat.

Kaja Staude

Journalist

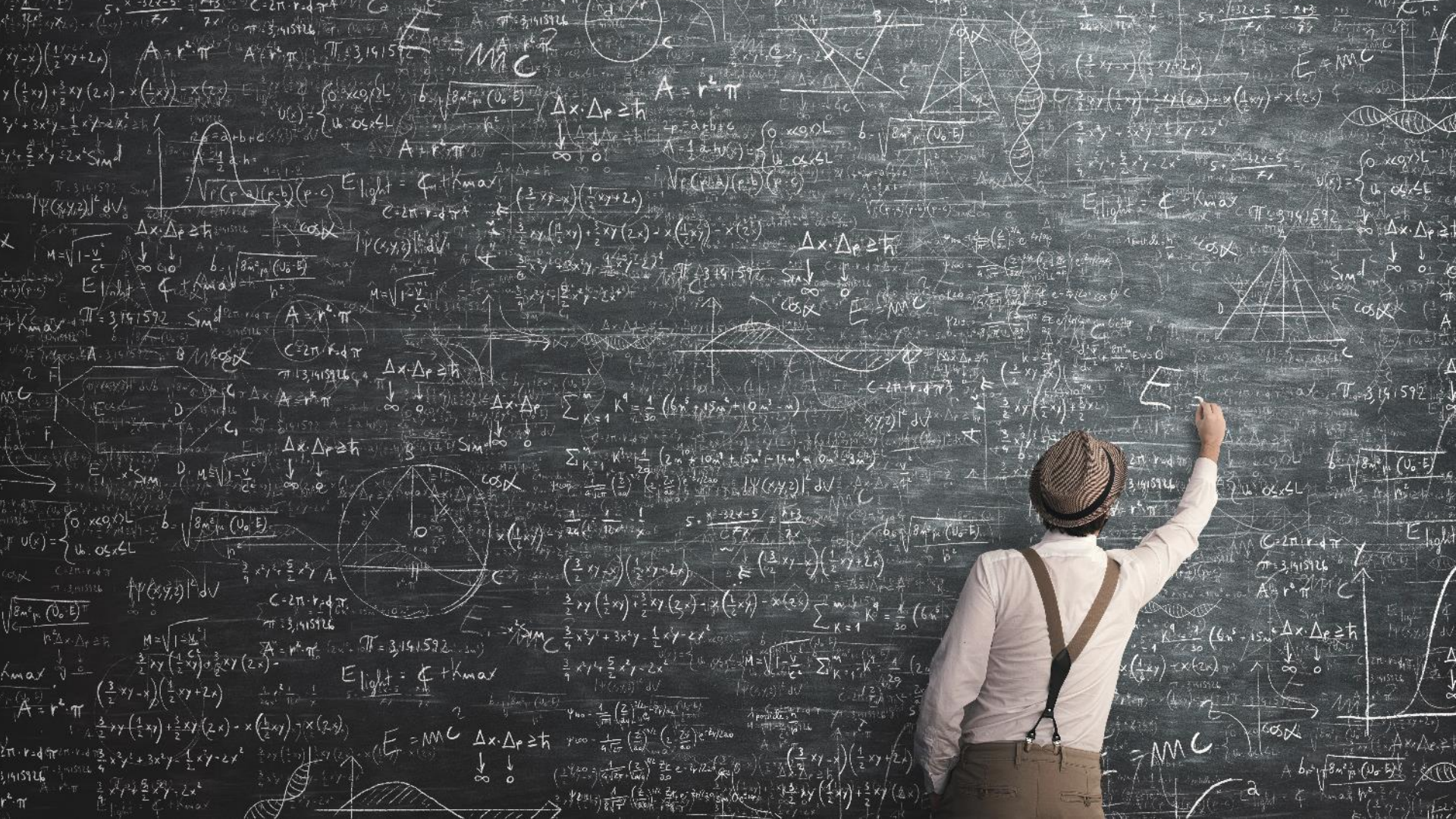
Publisert 16.

Oppdatert 18.

DATAANGREP

Norfund ble svindlet for 100 millioner: – Dette er dobbelt så stort som Nokas-ranet

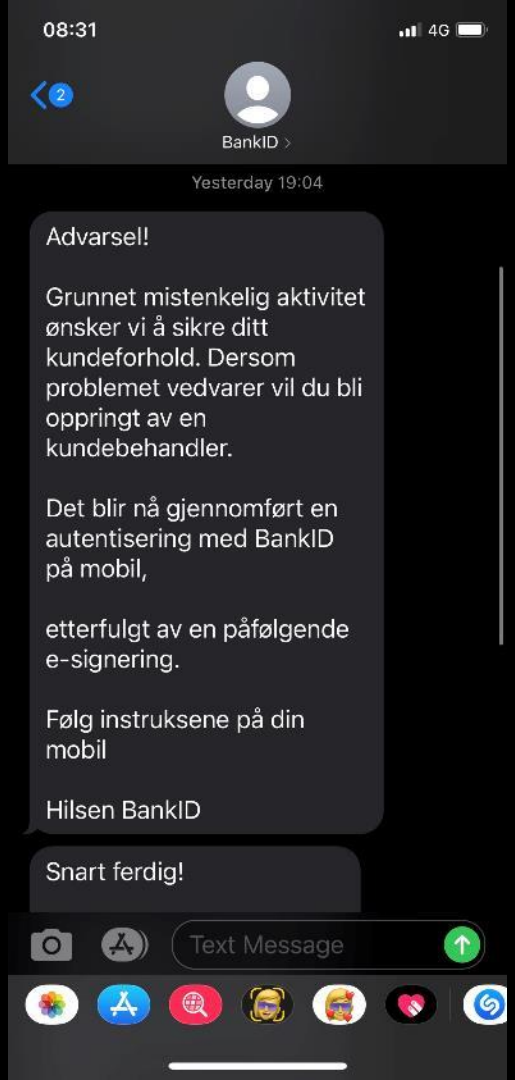
Det statseide Norfund har tapt 100 millioner kroner i et digitalt angrep, opplyser de

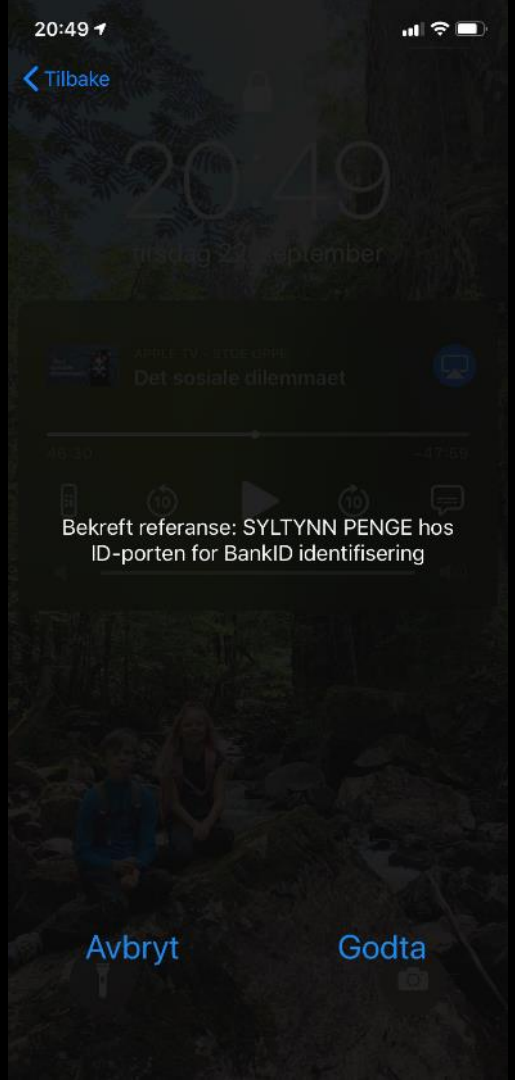


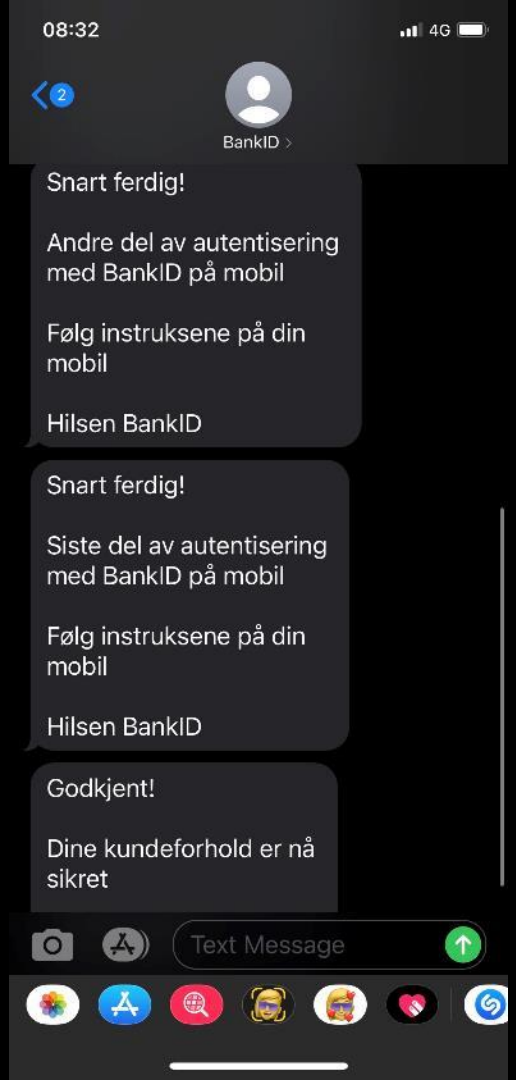

Statlige Aktører
Avanserte, Organiserte Kriminelle Grupper
Mindre Avanserte Organiserte Kriminelle Grupper
Bedrifter og Privat-personer

Dame (93) ble rundlurt av sleipe tyver: – Han var velkledd og hadde et nydelig skjerf

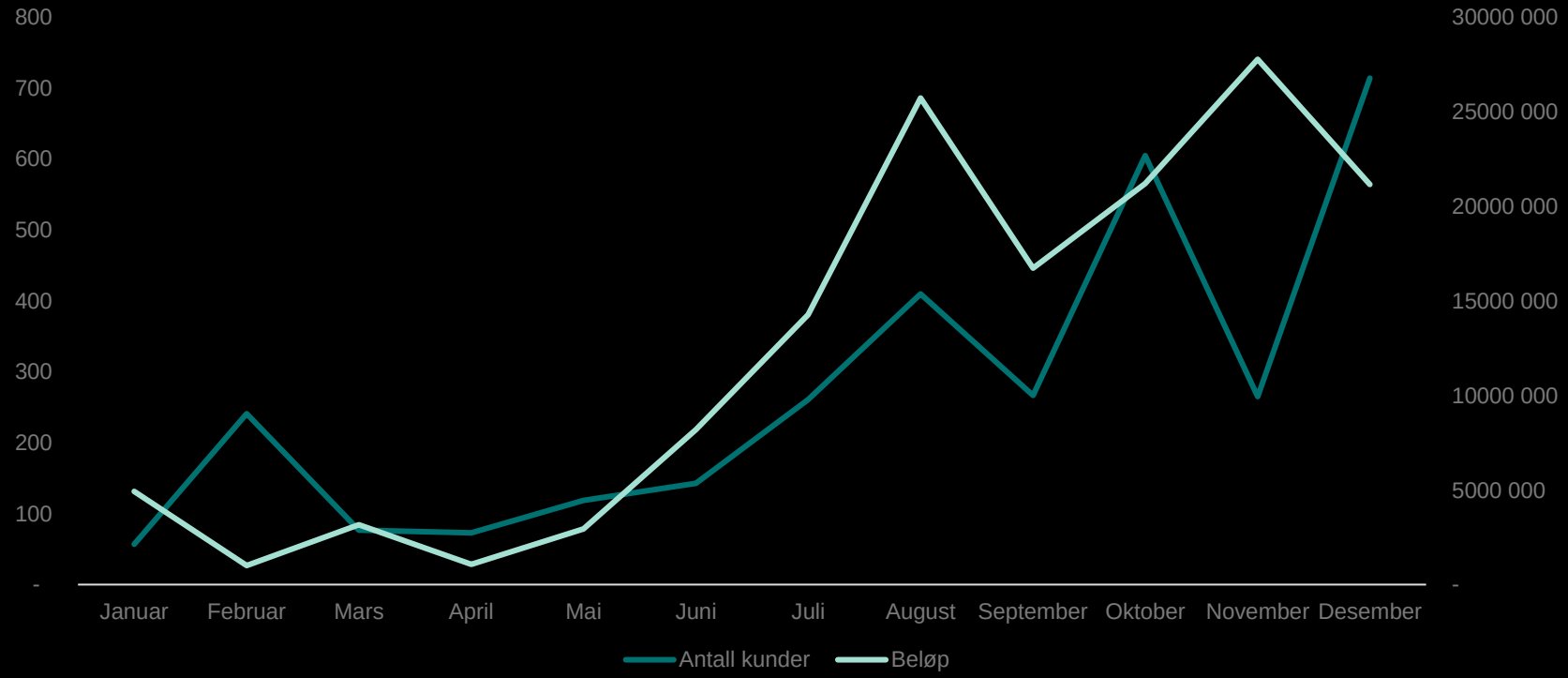

FAKE
OR
REAL?


08:31
4G
BankID
Yesterday 19:04
Advarsel!
Grunnet mistenkelig aktivitet ønsker vi å sikre ditt kundeforhold. Dersom problemet vedvarer vil du bli oppringt av en kundebehandler.
Det blir nå gjennomført en autentisering med BankID på mobil,
etterfulgt av en påfølgende e-signering.
Følg instruksene på din mobil
Hilsen BankID
Snart ferdig!
Text Message


20:49
Tilbake
Bekreft referanse: SYLTYNN PENGE hos ID-porten for BankID identifisering
Avbryt
Godta


08:32
4G
BankID
Snart ferdig!
Andre del av autentisering med BankID på mobil
Følg instruksene på din mobil
Hilsen BankID
Snart ferdig!
Siste del av autentisering med BankID på mobil
Følg instruksene på din mobil
Hilsen BankID
Godkjent!
Dine kundeforhold er nå sikret
Text Message

Saker 2021


800
700
600
500
400
300
200
100
-
30000 000
25000 000
20000 000
15000 000
10000 000
5000 000
-
Januar
Februar
Mars
April
Mai
Juni
Juli
August
September
Oktober
November
Desember
Antall kunder
Beløp


Compose
Inbox (0)
Outbox


ID theft

FC3 jobber for å begrense tap for DNB og kunder og opprettholde tilliten til konsernets produkter og tjenester

2021 oppsummert

DNB forhindret bedragerier for totalt 734 MNOK av en angrepssum på totalt 920 MNOK, alle bedragerier sett under ett

8393 saker håndtert (+ 66 %)

Organisert kriminalitet knyttet til bilfinansiering

73 anmeldelser inkl. **Massebedragerier**

109 % **flere kunder bedratt**

Stabilt antall **BEC** angrep

Antall grupperinger involvert i phishing har økt fra **3-5 til 15-20**

DNB phishing
Økt kvalitet og kvantitet

Lokale aktører involvert i flere av bedrageriene

Beløp forhindret i **BEC** saker økt med **180 %**

Antall kunder som har gått på phishing angrep har økt med **568 %**

33 % av org. krim miljøene involvert i hvitvasking er også involvert i bedragerier

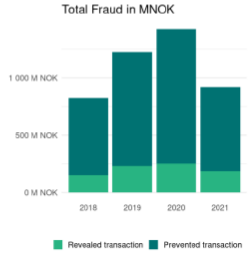
Digitale bedragerier har i perioden 2018 til 2020 økt med 300 %
Bedrageriene blir mer avanserte og holder høyere kvalitet

DNB

PUBLIC

Summary of 2021

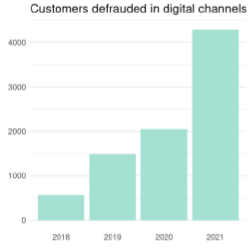
In 2021, FC3 handled 8393 fraud cases, an increase of 66 % from 2020. Out of these, 73 were reported to the police. The police reports include mass fraud, in particular large phishing campaigns and reporting of money mules. The number of police reports remains stable, but the complexity of the reported cases is high, and the investigations requires a lot of time. We are pleased to see that we have a good working relationship with the Norwegian police and that the police have acted in several cases.



When looking at the total amount of fraud, DNB managed to prevent a loss of **734 million NOK** (compared to 1 174 million NOK in 2020) out of a total of **920 million NOK** (compared to 1 425 million NOK in 2020) for the Group and our customers.

A reduction in the registered amount of fraud may be due to several different reasons. It is obvious that fraud volumes are greater than before, and for the dominating fraud category this year, phishing, the average amount attempted stolen is higher than before. One key reason for reduced numbers is a change in reporting on card fraud from one of our vendors. At the same time, banks are getting more effective in the fight against fraud and criminals are focusing on new payment channels outside bank infrastructure, exploiting opportunities given by PSD2 regulations and crypto currencies. This change will send some of the fraud outside our payment infrastructure and will therefore not be reported as cases with a specific amount attempted defrauded, but they might still be represented as cases without an amount. This could in part explain the rise in cases without a rise in amount the criminals have attempted to get away with. There will always be uncertainty in the total numbers and amount. This report only shows what DNB has registered within our infrastructure.

Digital fraud summary



The number of cases has increased by 65 % even though the amount attempted stolen has gown down by 34 %. The **number of defrauded customers in digital channels has increased by 109 %** from 2 051 to 4 289. The most significant change from the fraudsters was the increased quality, automation and the use of new communication channels and the finesse used in different phishing campaigns.

Manipulation happens over time, and the earlier we can intervene in an ongoing case, the lower the loss will be. This suggest that without intervention from DNB, other financial institutions and partners e.g., telecom companies, the stolen amounts would increase substantially.

Alle relevante trusselvurderinger påpeker at bedragerier er en av de kriminalitetsformen det er mest sannsynlig at vi vil bli offer for. Likevel erfarer vi en manglende digital tryggl og bevissthet rundt sikkerhet hos mange. Fraværet av bevissthet kan ses i sammenheng med manglende forståelse av problematikken og alvorligheten av dette samfunns-problemet. Bedragerier og annen internettkriminalitet utvikler seg stadig, og organiserte kriminelle grupper og terrorceller utnytter de store summene som finnes i økosystemen av økonomisk kriminalitet. Enten de gjør dette direkte, eller som et resultat av deres har med våpen, narkotika eller mennesker.

Som et resultat av digitalisering og globalisering har det blitt lettere å begå massebedragerier mot våre kunder. Videre utvikling av Internet of Things og økningen i antall datapunkter tilgjengelig vil gjøre oss enda mer sårbare i fremtiden, noe som vil fø til flere muligheter for bedragerier. Utviklingen viser at stadig flere organiserte grupperinger endrer sin virksomhet til å omfatte bedragerier mot privatpersoner og bedrifter, og DNB registrerer økende volumer på saker år etter år. Mange av våre bedriftskunder har etterspurt informasjon om råd for hvordan de kan redusere risikoen f å bli utsatt for målrettede angrep. Vi som bank kan ikke forhindre dette alene. Vi håper rådene i dette dokumentet kan bidra til å forebygge kriminalitet mot våre kunder.

Et viktig moment for å redusere faren for å bli utsatt for bedragerier er en sikkerhetskult som er forankret hos toppledelsen, der god e-postsikkerhet, aktive kontroller og sikkerhetstrening er verdsatt. Det er vesentlig at alle er kjent med faren for å bli utsatt fo falsk informasjon – bruk sunn fornuft og vær skeptisk.

En god kontroll er ikke et resultat av mistillit, men et uttrykk for god service.

Spørsmål?