POLITIET

MARS/NR1-2022

NYHETSBREV

Næringslivskontakt i Møre og Romsdal politidistrikt

Mulig arbeidslivskriminalitet

Andre uken i mars 2022 oversteg prisen på drivstoff 25 kroner literen flere steder i Norge. I forbindelse med de unormalt høye priser er det sannsynlig at en rekke bedrifter og transportfirma vil oppleve økonomiske utfordringer.

Norges Lastebileierforbund frykter konkursras som følge av den dramatiske økningen av drivstoffprisene. Useriøse aktører med økte utgifter kan benytte seg av alternative løsninger for å overleve.

Slike alternative "løsninger" kan være:

- Bedrifter og selskaper med normalt sett store drivstoffutgifter vil ved å tilby svarte tjenester fortsatt være konkurransedyktige i markedet.
- En drivstofftank på en lastebil kan romme 500 liter og kan ha en merkostnad på over kr. 2000 pr fylling av tank. En kan derfor i større grad oppleve tyveri av drivstoff, eller unndragelse av betaling.
- Nødvendige kostnadskutt i varebilbransjen kan føre til sosial dumping.

DIN KONTAKT I POLITIET

NÆRINGSLIVSKONTAKTEN

er politidistriktets hovedkontakt med næringslivet utenom straffesaksporet, og skal gi råd og videreformidle henvendelser til rett instans.

Kjell Arne Hestad

hestad@politiet.no

Telefon 926 06 045

Datainnbrudd og svindel

Mange bedrageri gjennomføres i dag ved bruk av internett, noe som har medført at de i større grad gjennomføres over landegrensene. Det er ikke uvanlig at bedrageren opererer fra et land, mens fornærmede befinner seg i et annet land, og transaksjonene skjer gjennom et eller flere tredjeland.

Datainnbrudd, identitetstyveri og sosial manipulering er bakenforliggende faktorer i flere av de ulike formene for bedrageri. Det menneskelige elementet er, og vil alltid være, sårbart for manipulering. Det er grunn til å tro at antall bedrageri er langt større enn anmeldelsestallene viser.

Politiet råder særlig bedrifter om å dobbeltsjekke betalingsopplysninger, særlig om de endres underveis, og verifisere disse mot en tidligere etablert kommunikasjonskanal. Man bør være ekstra på vakt om motpart forsøker å stresse eller gir uttrykk for hastverk i forbindelse med betaling.

For å unngå å bli bedratt, råder politiet at privatpersoner ikke skal gi fra seg personopplysninger, konto- og kredittkortinformasjon, passord eller pinkoder til personer og firmaer som henvender seg per telefon eller e-post.
Ved netthandel bør en sjekke hvorvidt informasjonen som gis er korrekt før en betaler for en vare eller tjeneste. Betal ikke for varer du ikke har bestilt.

Politiets råd er at bedrifter og privatpersoner tar det forebyggende arbeidet på alvor. Kunnskap, gode holdninger, tekniske sikkerhetstiltak og sunn fornuft anses å gi en betydelig gevinst.

Skulle ditt firma bli forsøkt svindlet, anbefaler vi å anmelde dette omgående.

Se for øvrig vedlagte Nødplakat!

Mobile vinningskriminelle - tyverier fra arbeidsplasser

Siste tida har vi hatt en økning av tyverier fra byggeplasser. Konteinere med dyrt verktøy, verdi på flere hundre tusen kroner, er stjålet.

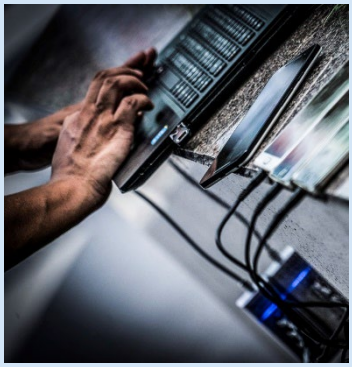
Fremgangsmåte:

- Rekognosering i forkant
- Innbrudd i konteinere og biler med verktøy som mål
- Klipping av hengelås og kutting av låsebeslag
- Utføres på kveld/natt, ofte inn mot helg
- Stjålet gods blir trolig fraktet til Østlandet for salg

Ta nødvendige forhåndsregler.

Tips politiet ved mistenkelig observasjoner!

SPOOFING



Spoofing er en teknikk som gjør at svindlere kan utgi seg for å kontakte deg fra et norsk nummer eller trygg IP-adresse. For å utføre spoofing på telefon bruker svindlerne en programvare som maskerer det originale nummeret de ringer fra. Dermed kan samtalen se ut som at den kommer fra et konkret norsk nummer, noe som ofte vekker mer tillit enn utenlandske numre. Den siste tiden har svindlere misbrukt nummeret til banker og politiet i bedrageri. Typisk i kombinasjon med sosial manipulasjon. Svindlere som praktiserer spoofing bruker både eksisterende og falske telefonnumre.

Hvis nummeret ditt skulle bli spoofet, betyr det ikke at mobilen din har blitt hacket, se ellers følgende lenker for mer informasjon om spoofing:

- https://www.telenor.no/sikkerhet/faq/hva-er-spoofing/
- https://www.telia.no/magasinet/tips/telefonsvindel-var-obs/

Hva en sperre medfører: En sperre som forhindrer spoofing er en faktisk sperre av nummeret som legges inn i sperrefilteret. Sperrefilteret gjør at et nummer ikke kan sette opp samtaler fra land utenfor Norge til norske nummer med prefiks +47, det samme gjelder hvis samtalen originerer (starter) i Norge og blir rutet via utlandet.

Sofistikert og godt planlagt

mot virksomheter som skal kjøpe pumper av «Vattenfall»

Nordea melder om noen saker i november med et modus som fremstår som sofistikert og godt planlagt som har berørt deres kunder i Norge. En annen nordisk bank har hatt tilsvarende saker med samme modus den siste tiden som har berørt kunder i Norge og Danmark.

Moduset er slik: Kunde (bedrift) mottar en e-post som utgir seg for å være det svenske selskapet Vattenfall med en bestilling av en spesifikk type pumpe (typ oljeindustri, energi industri e.l). Informasjon tyder på at det i denne forespørselen blir opplyst om hvor denne spesifikke pumpen kan kjøpes og Nordeas kunde kjøper da inn pumpen/ flere pumper av samme slag i henhold tilordre og betaler for disse (ofte i britiske pund til Storbritannia på bakgrunn av en proforma faktura fra leverandøren). Beløpene har vært på opptil 50 000 pund per kunde. Pumpene blir ikke levert og det viser seg at leverandøren de har blitt bedt om å kjøpe av er falsk, noe som betyr at svindlerne opererer både som de som forespør pumpen («Vattenfall») og som leverandør av pumpen i den andre enden. For den falske leverandøren er det etablert falske internettsider for å underbygge legitimiteten til leverandøren.

Et annet aspekt i dette moduset er at det også har vært benyttet Search Engine Optimisation poisoning, som betyr at dersom mottakende selskap av kjøpsordre «googler» produktnavnet så kommer internettsiden til den falske leverandøren av pumpen frem som øverst på søkeresultatet.