forslag om å innføre grunnrenteskatt på havbruk til havs. Utredningen må gi en avklaring om det er grunnlag for grunnrente på havbruk til havs.

- Stortinget ber regjeringen innføre en ordning som gjør at redusert produksjon som følge av trafikklyssystemet, kan produseres i lukket teknologi.
- Stortinget ber regjeringen legge frem forslag om en miljøteknologiordning i løpet av 2023.
- Stortinget ber regjeringen i løpet av våren 2024 legge frem en sak om bedre organisering av samarbeidet mellom myndigheter og oppdrettsnæringen for å sikre en mer helhetlig forvaltning, bedre bærekraft og bedre fiskevelferd.
- Stortinget ber regjeringen i løpet av våren 2024 legge frem tiltak for økt bearbeiding av sjømat i Norge.
- Stortinget ber regjeringen sikre at Havbruksfondet tilføres midler som om produksjonsavgiften ble økt fra 56 øre til 90 øre fra 1. januar 2023.

Svindel i en digital hverdag

Vi hører nesten daglig om ulike virksomheter og privatpersoner som har blitt rammet av ulike former for digitale svindler. Den stadige utviklingen i samfunnet gjør det mer krevende å verne seg mot potensielle digitale trusler og svindelkampanjer.

Legal & Privacy Officer
Andreas Forbech Havre
Intility

Den digitale utviklingen gjør det ikke bare enklere å effektivisere svindelforsøk, men også å tilpasse svindelen til det enkelte offeret. Graden av profesjonalitet og kompleksitet blant ondsinnede aktører er varierende. På den ene siden har du svindelforsøk som er enkle å avsløre, mens du i den andre enden finner organiserte aktører som selger informasjon som brukernavn og passord eller påtar seg oppdrag for å utføre løsepengeangrep.

Enklere å utforme troverdig innhold

Svindelforsøk pr. epost kunne tidligere gjerne gjenkjennes på bakgrunn av dårlig språk, men nye tjenester bidrar til å gjøre det stadig enklere å utforme innhold som fremstår som troverdig og som det er krevende å avsløre som potensiell svindel. DNB kan fortelle at de har sett en økning på 45 prosent i antall svindelforsøk som de har behandlet i 2022 sammenlignet med 2021. Sammenlignet med 2020 er økningen på 1000 prosent. Finanstilsynet har rapportert om færre angrep på finansiell infrastruktur i 2022, men mener likevel at omfanget av digital kriminalitet med konsekvenser for finanssektoren synes å øke.

AI-tjenester på nett

Det har vært mye oppmerksomhet rundt ChatGPT, Dale-E og andre AI-tjenester på nett. Språkmodellen ChatGPT har hatt en enorm vekst i antall brukere. Mens Spotify, Facebook og Netflix brukte henholdsvis 5, 10 og 42 måneder på å nå én million brukere, brukte ChatGPT fem dager. Det er estimert at det tok tre måneder før tjenesten fikk 100 millioner månedlige aktive brukere. Nye og eksplosive trender som dette blir gjerne utnyttet av aktører med onde hensikter. Tilsvarende så man for kryptovaluta og Bitcoin. AI-trenden kan utnyttes på flere måter. Svindlere kan ta i bruk AI som et verktøy for å forbedre svindelen ved at tjenesten kan brukes til å utforme phishing e-post på et gitt språk og i en gitt kontekst, eller automatisere og forenkle utnyttelsen av sårbarheter.[1]

Utnytter etterspørselen etter AI-tjenester

Det er allerede avslørt tilfeller hvor ondsinnede aktører utnytter selve etterspørselen etter AI-tjenester. Dette kan for eksempel være tjenester som utgir seg for å være ChatGPT, men som i realiteten er en kopi. For brukerne kan den fremstå og fungere likt, men i bakkant kjører det prosesser som har andre formål. Disse kan for eksempel prøve å stjele informasjon eller installere programvare på brukerens maskin.

I mange tilfeller er det ikke tydelig for offeret hvordan svindleren kan få en økonomisk vinning av handlingen. Dette

1 Security Implications of ChatGPT, Cloud Security Alliance, https://cloudsecurityalliance.org/artifacts/security-implications-of-chatgpt/

TIPS

- Ikke trykk på lenker du får tilsendt. Er du usikker på om det er en reell henvendelse bør du gå til den aktuelle nettsiden selv og logge inn der.
- Vær årvåken, selv om henvendelsen virker å være tilpasset deg.
- Opplever du mistenkelig aktivitet bør du ta kontakt med din IT-leverandør. De kan hjelpe deg med å foreta nærmere undersøkelser av aktiviteten.
- Er du i tvil om en henvendelse er reell, ta kontakt med avsender på en annen måte enn de kontaktet deg på.
- Bruk gode og unike passord og aktiver totrinnsbekreftelse (MFA) på alle kontoer. Vurder om du burde ta i bruk en passordbank (password manager).
- Hold enhetene dine oppdatert. Dette beskytter mot sårbarheter i operativsystemet og programvaren.
- Ikke åpne e-poster eller vedlegg med mindre du er trygg på avsenderen.

gjør det vanskeligere å avsløre svindelforsøket ettersom brukeren er mindre årvåken enn hun ville vært hvis hun mottok en forespørsel om å logge inn med BankID. Likevel er det viktig å alltid være bevisst på hva man gjør, og hvem man samhandler med. En aktivitet som i seg selv virker uskyldig, kan være et ledd i en lengre prosess, for eksempel å samle mer generell informasjon som senere kan brukes for å fremstå mer troverdig i forbindelse med et svindelforsøk.

Meldinger fra en «bekjent»

Det er avdekket at en utvidelse til Chrome, som utga seg for å være en offisiell ChatGPT-utvidelse, i bakkant forsøkte å ta over brukerens Facebook-konto. Svindlere med tilgang til noens Facebook-konto vil lettere gjennomføre mer overbevisende svindelforsøk mot vedkommendes venner. Svindleren kan for eksempel se at vedkommende snart skal delta i et privat arrangement. Noen dager etter arrangementet kan svindleren sende ut melding med link til de andre deltakerne med beskjed om at de der kan laste ned bilder fra arrangementet. Når meldingen kommer fra en bekjent og knytter seg til et arrangement som nylig har funnet sted, blir det krevende å oppdage svindelen. Blant vår kundemasse har vi også erfart at utenforstående kontakter ansatte hos våre kunder og utgir seg for å ringe fra oss, deres IT-leverandør.

Lekkasjer

En svindler er likevel ikke avhengig av å ta over noens kontoer på sosiale medier for å samle informasjon til en mer personlig tilpasset form for svindel. Mye informasjon ligger tilgjengelig på internett, både lovlig og ulovlig publisert. I løpet av de siste ti-årene har flere store nettjenester blitt utsatt for angrep. Lekkasjer fra disse angrepene har gjort at millioner av brukernavn og passord er tilgjengelige på internett.

Venter på det riktige øyeblikket

En tålmodig svindler venter gjerne på det rette tidspunktet til å iverksette svindelen. Dette kan være tilfelle når svindleren i første omgang får tilgang til en e-postkonto og oppretter en videresendingsregel. En slik regel vil sørge for videresending av all e-post til offerets konto til en e-postkonto valgt av svindleren selv. Svindleren kan da følge med på aktiviteten, og vente på riktig øyeblikk å slå til. Når svindleren for eksempel ser at det inngås en avtale mellom offeret og en leverandør, hopper de inn i samtalen og utgir seg for å være leverandøren som oppgir betalingsinformasjon.

Vær proaktiv

Etter hvert som teknologien utvikler seg, vil også svindlerens metoder følge etter. Ondsinnede aktører er gjerne tidlig ute med å benytte seg av nye verktøy og trender som kan forbedre deres metoder og bedre tjene deres formål. Det digitale trusselbildet er komplisert, hvor både statlige og kriminelle aktører utfører angrep. Selv om stadig flere får et aktivt og bevisst forhold til IT-sikkerhet, ser vi fortsatt at en del velger å ikke gjennomføre tiltak før det er for sent. For å unngå at man blir et offer for svindel, er det derfor viktig å ha et bevisst og proaktivt forhold til IT-sikkerhet. Et greit sted å starte kan være å kartlegge sannsynligheten for og konsekvensene av ulike angrepsscenarioer. Deretter bør det undersøkes hvilke tiltak som kan bidra til å øke sikkerheten på disse områdene.

En tålmodig svindler venter gjerne på det rette tidspunktet til å iverksette svindelen.