Ny falsk epost som linker til AutoInvoice

Vi viser til tidligere advarsler (se under) om falske e-poster som utgir seg fra å være fra Visma, som viser til falske påloggingsider.

Vi har blitt gjort kjent med at det er en ny falsk e-post i sirkulasjon og ønsker herved å varsle om dette. Vi vil understreke at disse e-postene kommer ikke fra Visma, de er forsøk på svindel. Det er viktig at man som mottaker av en slik e-post ikke følger linker eller andre instruksjoner i denne.

Svindel e-posten har tekst som dette:

"Fra: Visma Autoinvoice <do.not.reply@visma.com>
Sendt: 17. april 2018 10:01
Til:
Emne: Vennligst bekreft kontoen din | Visma Autoinvoice
Under vår regelmessige planlagt vedlikehold og verifisering av kontoer har vi forbedret kontosikkerheten din.
- For å beskytte kontoen din, tofaktorautentisering er tatt i bruk.
- Dette er et ekstra sikkerhetslag laget for å forhindre uautorisert tilgang til kontoen din.
Vennligst logg inn og oppdater kontoprofilen din umiddelbart; <her var det en link du ikke må besøke>.
Hvis kontoinformasjonen din ikke oppdateres innen 48 timer, så vil din evne til å få tilgang til kontoen din være begrenset.
Kom i gang <her var det nok en link du ikke må besøke> .Hvis du har spørsmål, bruker du Supportpanelet i Visma.net <her var det en tredje link du ikke må besøke> .
Godkjenning mens du er på farten?
Bruk Visma Manager app som du kan laste ned gratis fra Apple App Store og Google Play.
Vennlig hilsen
Visma"

Dersom du allerede har besøkt noen av disse linkene og angitt brukernavn og passord der må du umiddelbart bytte ut passord alle steder hvor du har benyttet passordet du tastet på den falske siden. Dersom du har avgitt passord til din e-post server, så begynn med å endre dette slik at uvedkommende ikke kan få tilgang til din mailkonto. Deretter kan du endre passord andre steder.

Dersom du oppdager falske fakturaer sendt fra din konto, andre uregelmessigheter eller har spørsmål, vennligst ikke nøl med å kontakte Visma via ditt ordinære supportsenter, via chat på community, telefon: 09101 eller e-post: kundesenteret@visma.no.

Dersom du har mottatt e-post som nevnt over, vil vi sette pris på om du kunne fortelle oss om det, for eksempel videresende til kundesenteret@visma.no, slik at vi får ytterligere hjelp i å spore kilden til dette svindel-forsøket.

Vennlig hilsen
Visma

Kopi av tidligere sendt epost:

Visma har avdekket at noen utenforstående har spredt falske e-poster, med hensikt å få tilgang til brukernavn og passord for tjenesten Visma AutoInvoice.
De falske e-postene som tilsynelatende ser ut til å være sendt fra Visma, viser som avsender: approval.do.not.reply@visma.com

Vi vil understreke at disse e-postene kommer ikke fra Visma, de er forsøk på svindel. Det er viktig at man som mottaker av en slik e-post ikke følger linker eller andre instruksjoner i denne.

De falske e-postene har tekst som dette:

“Du har en eller flere godkjenningsoppgaver som trenger din oppmerksomhet. For mer informasjon, logg inn på <link som pekte på en falsk innloggingsside>.
Du kan endre innstillingene for hvordan du mottar meldinger under Innstillinger - Mine innstillinger - Mine e-postinnstillinger.
Hvis du har spørsmål, bruk Supportpanelet i Visma.net.
Godkjenne mens du er på farten?
Bruk Visma Manager app som du kan laste ned gratis fra Apple App Store og Google Play.
Vennlig hilsen,
Visma”

Vi fjernet for en stund siden alle linker i e-poster fra Visma.net Approval, nettopp for å unngå situasjoner som dette. E-poster fra Approval vil ikke inneholder linker.

Dersom du eller en kollega allerede har du forsøkt å logge på via den falske siden, må du umiddelbart endre ditt passord i tjenesten Visma AutoInvoice. Du bør gjøre følgende:

1. Logg inn på AutoInvoice, Klikk på innstillinger oppe til høyre, Klikk på "Endre passord" nede i menyen til venstre. Du kan eventuelt bruke “Glemt passord” funksjonen på innloggingssiden.
2. Du må også sjekke om det er opprettet nye brukere som du ikke kjenner til. Det gjør du ved å gå til Innstillinger oppe til høyre og klikk på Brukere. Eventuelle uautoriserte brukere må slettes, men koordiner med admin bruker dersom det ikke er deg.
3. Når du har endret passord må du resette API nøkkelen din for å hindre mulig fremtidig misbruk av denne. Dersom det er din API nøkkel som brukes av integrerte systemer hos dere, må du sjekke hvordan du oppdaterer API nøkkel i systemene hos deg som er integrert mot AutoInvoice.Ta eventuelt kontakt med support for aktuelt system.

4. Deretter; gå til Innstillinger, Personlige innstillinger, Detaljer og trykk reset API nøkkel. Så limer du inn den nye API nøkkelen der den skal angis i integrert systemer.
5. Dersom du trenger hjelp eller mer informasjon, vennligst kontakt din support kanal for det integrerte system.

Vi bør også sjekke dine sendte fakturaer. Dersom du oppdager falske fakturaer sendt fra din konto, andre uregelmessigheter eller har spørsmål, vennligst ikke nøl med å kontakte Visma via ditt ordinære supportsenter, via chat på community, telefon: 09101 eller e-post: kundesenteret@visma.no.

Dersom du har mottatt e-post som nevnt over, vil vi sette pris på om du kunne fortelle oss om det, for eksempel videresende til kundesenteret@visma.no, slik at vi får ytterligere hjelp i å spore kilden til dette svindel-forsøket.

Vennlig hilsen
Visma