St1 Finance Oy (AS) – sikkerhetsveiledning 11/2018

Denne sikkerhetsveiledningen inneholder instruksjoner for sikker bruk av betalingstjenestene fra St1 Finance Oy (AS). Følg disse instruksjonene når du bruker tjenestene. Les denne veiledningen nøye og se ytterligere informasjon om emnet: **www.st1finance.no**. **Kundeserviceavdelingen på telefonnummer +47 22 66 53 20** hjelper deg med beskyttelse av informasjonen din når du bruker betalingstjenesten, og gir deg hjelp med potensielle problemer.

Husk at St1-betalingskontoen og de relaterte betalingsinstrumentene, informasjon om betalingsinstrumentene, tilgangskodene og PIN-kodene er personlige. Alt dette må oppbevares og brukes på en forsiktig og trygg måte, slik at ingen uautoriserte personer, inkludert medlemmer i din egen familie, kan finne ut av eller bruke dem. Hvis du har lastet ned en mobilapp for telefonen og lagt til betalingstjenestefunksjoner, må du håndtere telefonen med like stor forsiktighet som alle andre betalingsinstrumenter.

Sikker bruk av betalingsinstrumenter og PIN-koder:

Du må alltid oppbevare betalingsinstrumentet og nummeret og PIN-koden for betalingsinstrumentet separat.

Lær deg tilgangskoden og PIN-koden for tjenesten utenat. Ikke skriv ned tilgangskoden eller PIN-koden eller lagre dem i et enkelt identifiserbart format. Du må heller ikke lagre kodene på mobiltelefonen eller oppbevare dem i vesken eller lommeboken eller andre steder sammen med betalingsinstrumentet.

Avhengig av omstendighetene bør du regelmessig kontrollere at betalingsinstrumentene og mobiltelefonen er trygge, spesielt hvis det er stor risiko for å miste dem.

Når du betaler med betalingskortet ditt, må du skjule tastaturet når du taster inn PIN-koden til kortet. Dette hindrer at uautoriserte personer ser koden din.

Når du bruker betalingstjenesten og oppgir tilgangskoden til tjenesten eller annen lignende informasjon på telefonen eller datamaskinen, må du skjule tastaturet slik at uautoriserte personer ikke kan se opplysningene.

Ikke bruk en betalingsterminal eller -maskin hvis området ikke føles trygt. Bruk heller ikke tjenesten på mobiltelefonen hvis du ikke føler deg i trygg der du befinner deg.

Send aldri informasjon om betalingsinstrumentet eller -tjenesten, tilgangskoden eller PIN-koden via e-post eller over telefon. Oppgi aldri personlige opplysninger, for eksempel passord eller kortdetaljer, når du har kontakt med venner eller familie på sosiale medier.

Uansett betalingsmåte må du alltid huske å dobbeltsjekke totalbeløpet før du godkjenner et kjøp. Du kan enkelt overvåke kjøp som gjøres med kortet, ved hjelp av kvitteringer, bankutskrifter og fakturaer.

St1 kommer aldri til å be deg bytte til en nettbasert tjeneste eller en annen selvbetjent kanal via en kobling i en e-postmelding, eller be deg om å oppgi tilgangskoder, PIN-koder eller informasjon om betalingsinstrumenter via e-post eller over telefon. Hvis du får en mistenkelig e-postmelding der St1 ser ut til å være avsender, må du umiddelbart rapportere dette til St1s kundeservice: + 47 22 66 53 20 (døgnåpen). Vær alltid på vakt mot uventede e-postmeldinger som tilsynelatende kommer fra en organisasjon med godt omdømme, for eksempel en bank, skattemyndighetene eller en nettbutikk. Ikke klikk på noen av koblingene i meldingen.

Vær forsiktig når du handler på Internett. Ikke oppgi kortopplysningene dine med mindre du skal kjøpe noe.

Kontroller at nettbutikken oppgir kontaktinformasjon i tilfelle potensielle klager (telefonnummer eller e-postadresse til kundeservice, bedriftens postadresse osv.).

Instruksjoner for å hindre nettsvindel:

Oppdater enhetens programmer regelmessig, og hold alltid datamaskinens brannmur oppdatert.

Installer et antivirusprogram og oppdater det regelmessig. Installer også en antivirusapp for mobiltelefonen hvis tilgjengelig.

Nettbetalinger

Når du handler på nettet, må du sørge for at tilkoblingen din er kryptert (nettleserens adressefelt viser «https»). En kryptert tilkobling er vanligvis angitt med et lås- eller nøkkelsymbol.

Kontroller alltid vilkårene og betingelsene for levering og retur i nettbutikkordren, og ta vare på ordrebekreftelsen.

Hvis du bestiller en løpende (for eksempel månedlig) tjeneste fra en nettbutikk, må du alltid finne ut på forhånd hvordan du kan avslutte eller kansellere kontrakten, og når betalingen for tjenesten avsluttes.

Ta vare på all dokumentasjon som er knyttet til kjøpet ditt. Det kan hende du får bruk for det, for eksempel som kjøpsbevis eller for å finne vilkårene og betingelsene for salget.

Vær på vakt mot fristende tilbud og andre opplysninger på Internett hvis disse virker for gode til å være sanne.

Sikker bruk av tjenester på nettet og på mobilenheter

Hold programvaren og operativsystemet på enheten (datamaskinen, telefonen eller nettbrettet) oppdatert.

Beskytt enheten mot skadelig programvare ved hjelp av antivirus- og brannmurprogramvare. Oppdater programvaren regelmessig i henhold til produsentens instruksjoner.

Hvis du lagrer eller bruker betalingsinstrumentet på en ekstern tjenesteleverandørs lommeboktjeneste eller lignende, krever vi at enheten låses ved hjelp av for eksempel en kode eller fingeravtrykk.

Ikke la noen registrere fingeravtrykk, ansikt eller annen biometrisk identifikator til enheten som kortet ditt er registrert på, fordi det tillater deg å godta betalingstransaksjoner ved hjelp av på kortet ditt, ved bruk av Apple Pay-appen eller lignende betalingsmåter.

Logg alltid av tjenesten når du er ferdig med å bruke nett- eller mobilappen.

Sperring av tjenesten

Tlf. + 47 22 66 53 20

Hvis du mister eller blir frastjålet betalingskortet, tilgangskoden, PIN-koden eller telefonen som du bruker St1 Mobile på, må du umiddelbart hindre bruk av disse ved å ringe tjenesten for sperring.