Utbildningsunderlag

PCI-DSS TVM

VÄSTTRAFIK – EN DEL AV VÄSTRA GÖTALANDSREGIONEN

västtrafik

Skydda kortdata

Syfte

- Säkerställa att kundernas kortdata skyddas.

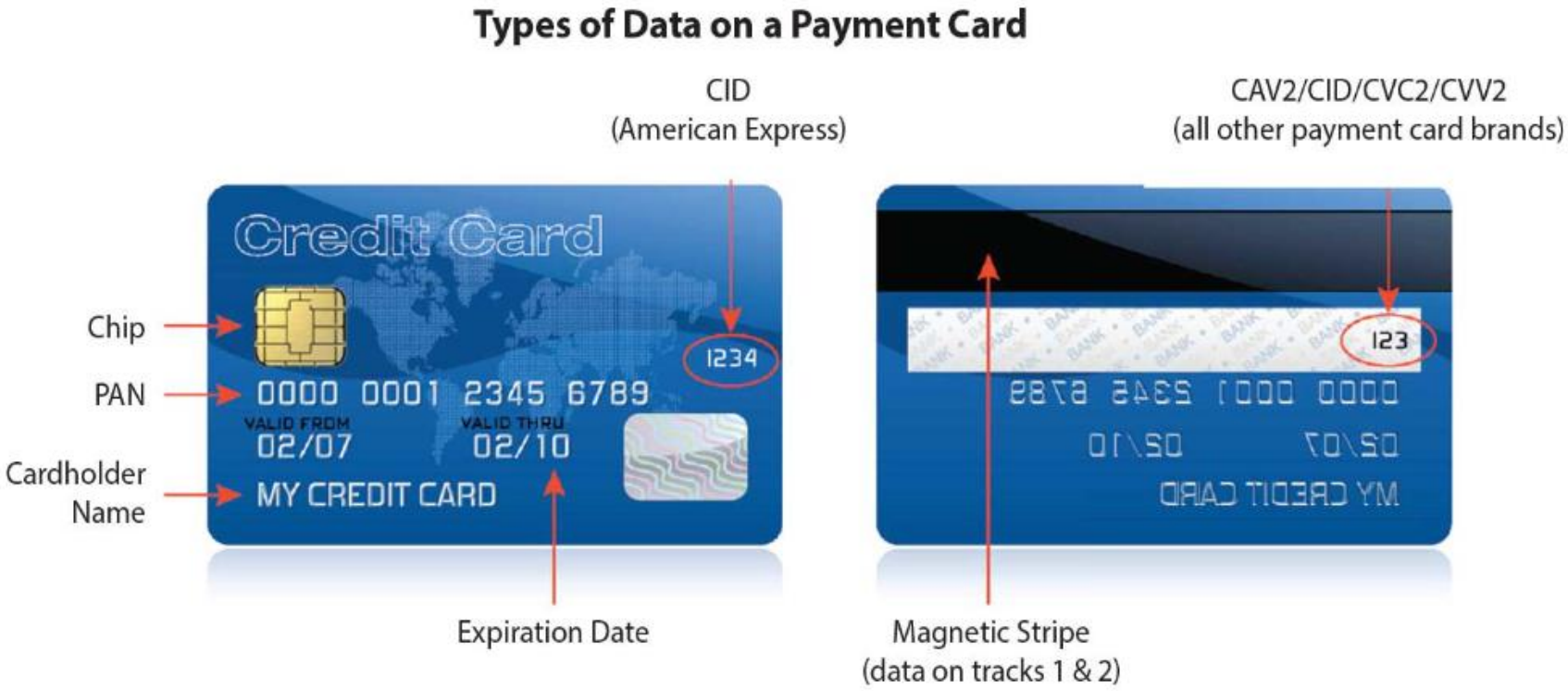
Innehåll

- Vad är kortdata?
- Varför behöver kortdata skyddas?
- Hur skyddas kortdata?

västtrafik

Vad är känslig kortdata?

Kortdata är stöldbegärlig information. Genom att få tag på Account Number (PAN) och övrig känslig autentisieringsdata såsom CVV-kod kan en tjuv använda kortet som sitt eget.



Kortdata

Ett betal- eller kreditkort kan användas på två sätt när det handlar om betalning för varor och tjänster.

1. Du kan använda magnetremsan eller chippet på kortet. Här finns lagrade data som används för att identifiera kortet. När du drar kortet i kortläsaren i kassan läser kortläsaren av uppgifterna och använder dem för att kommunicera med kortutgivaren och banken.
2. Du kan använda de uppgifter som finns tryckta eller präglade på kortet.

västtrafik

Carding och skimning

För 100 år sedan var tjuvarna ficktjuvar. Idag används mestadels mer avancerade tillvägagångssätt för att lura av andra personer deras pengar. Två metoder som är inriktade mot bankkort och kreditkort av olika slag är carding och skimning.

- Carding är tekniker och metoder för att använda kortets synliga information i bedrägligt syfte.
- Skimning är tekniker för att läsa av informationen på kortets magnetremsa.

västtrafik

Carding

Carding är en samlande benämning på alla slags tekniker i vilka kortets synliga information används olovligen. Bedrägerierna genom carding har ökat kraftigt under de senaste åren. Carding är vanligt och för dig som kortinnehavare gäller det att vara försiktig med hur du använder dina kortuppgifter.

För att utföra ett bedrägeri genom carding behövs normalt tre uppgifter:

- kortnumret
- CVC-koden
- kortets giltighetsdatum

På vissa webbplatser med en mycket dålig säkerhet räcker det emellertid med enbart kortnumret.

västtrafik

Komma åt kortuppgifter

På Internet sker en omfattande handel med stulna kortnummer. Ett annat sätt att komma åt kortuppgifter i bedrägerisyfte är att använda tekniker för nätfiske, eller phishing med ett annat namn. En vanlig metod för nätfiske är falska webbplatser som uppmanar besökarna att lämna sina personliga data och sin kortinformation.

västtrafik

Skimning

Skimning = kortkapning.

Skimning sker genom att en speciell avläsare monteras på terminalen som registrerar allt som görs.

Vissa skimningsverktyg kopierar endast innehållet på magnetremsan på kortet medan andra även registrerar vilken PIN-kod som slås in.

Om endast magnetremsan kopieras är syftet främst att handla varor och beställa tjänster på nätet. I det sistnämnda fallet får bedragaren all den information som behövs för att skapa ett falskt kort som kan användas för att ta ut pengar på kortet.

västtrafik

Skimning – så här går det till

- En avläsningsanordning (sniffer device) sitter inne i terminalen och används för att fånga upp och logga trafiken från terminalen.

- Ficktjuvar tjuvkikar över axeln och tar reda på PIN:en och stjäl sedan kortet.

- Overlay attack 1 – En extra kortläsare installeras ovanpå ordinarie kortläsare. Dessutom installeras en kamera vid PIN skyddet eller i taket.

- Overlay attack 2 - En extra kortläsare installeras ovanpå ordinarie kortläsare. En extra PIN keyboard installeras ovanpå ordinarie PIN keyboard.

västtrafik

Hur skyddar vi oss?

Se till att vi uppfyller kraven för PCI DSS (Payment Card Industry Data Security Standard).

Syftet med PCI är att säkerställa att alla som hanterar kortinformation gör det på ett sådant sätt att obehöriga inte kommer åt informationen.

Den som tar betalt med kort har ansvar för att skydda kortinformationen så att den inte blir tillgänglig för obehöriga.

västtrafik

Payment Card Industry Data Security Standard

Payment Card Industry Data Security Standard (PCI DSS) är en säkerhetsstandard framtagen av bland andra Visa och MasterCard. Innehållet i standarden hanteras av PCI Security Standards Council.

Standarden omfattar 6 huvudområden:

- Säkerheten i nätverket
- Skydda kortinformationen
- Skydd mot sårbarheter
- Behörighetskontroll
- Övervakning och test samt
- Användning av säkerhetspolicy

västtrafik

Hur skyddar vi oss?

Kortbedrägeri kan undvikas om:

- Personalen har information om hur de skiljer på en modifierad terminal mot en orginalterminal.
- Kortanvändaren informeras om att skydda sin PIN.
- En bild på terminalen i orginalutförande finns bredvid terminalen för att både kortanvändare och personal lättare ska kunna upptäcka misstänkt bedrägeriförsök.
- Kortanvändaren upplyses om att skydda sin PIN genom att exempelvis täcka för inmatningen med handen eller kroppen.
- Personal kontrollerar terminalen regelbundet.

västtrafik

CHECKLISTOR/PROTOKOLL

västtrafik

Tack!