

CYBERBROTT – SNART VARJE FÖRETAGARES VARDAG



Svensk Handel

CYBERBROTTLIGHETENS OMFATTNING OCH KOSTNADER

- Antalet anmälda bedrägerier ökade med 100 % mellan 2010 - 2020
- Anmäldes närmare 200 000 brott förra året
- IT-brottsligheten genererade 2 miljarder i brottsvinster förra året – motsvarar de sammanlagda vinsterna av narkotikaförsäljning i Sverige
- Snart världens 3e största ekonomi efter USA och Kina – beräknas omsätta mer än 10 biljoner dollar årligen 2025
- Brottsligheten finansierar till stora delar den grova organiserade brottsligheten

UTSATTHETEN BLAND HANDELSFÖRETAGEN



- 60 procent har mottagit ett falskt mejl, sms eller telefonsamtal

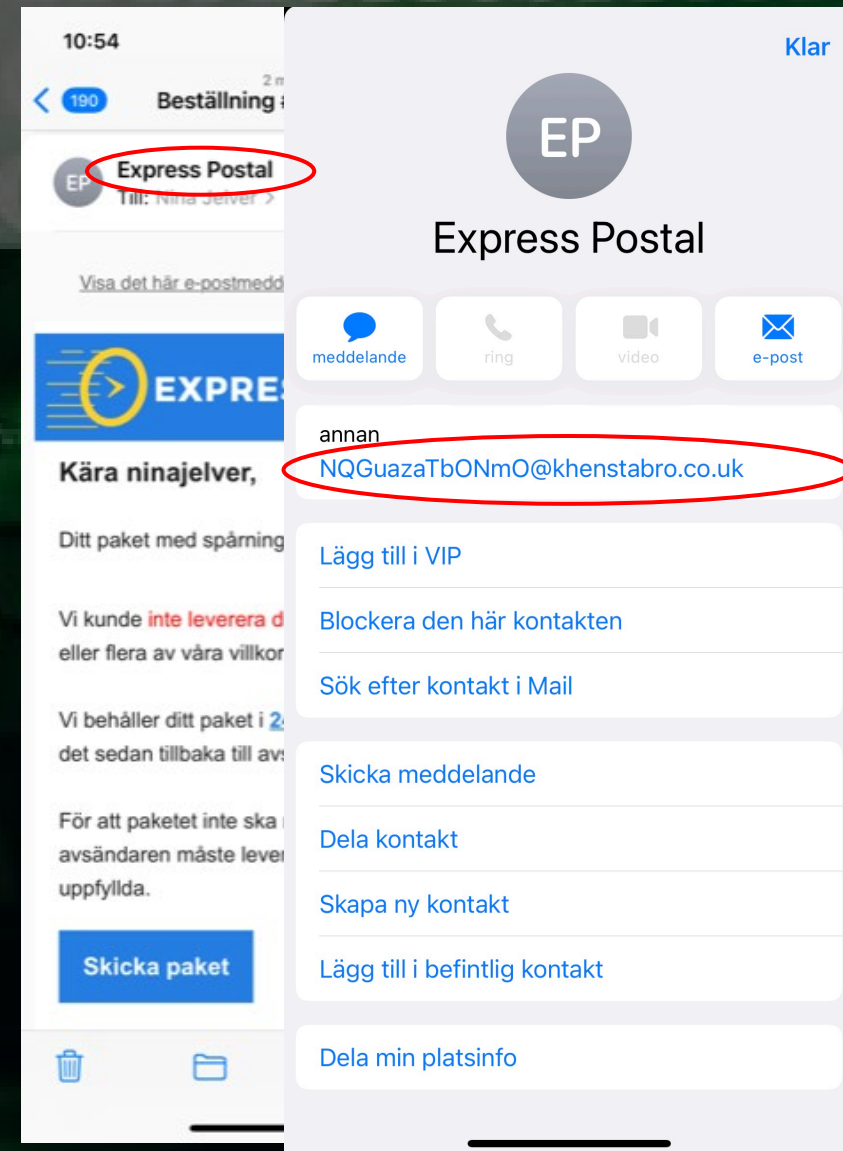
- 48 procent har fått en bluffaktura

- 46 procent har fått förfalskade mejl där avsändaren ser ut att vara en kollega eller chef

- 23 procent har drabbats virus eller skadlig kod

PHISHING- SMISHING - VISHING

- Omdirigering till en sida där man uppges lämna ifrån sig kortuppgifter
 - Kontakta banken och spärra kortet
- Ofrivilligt och ovetandes ingår prenumerationer
 - Bestrid om vilseledande
- Nedladdning av skadlig kod (ransomware)
 - Ta hjälp - betala inte!



BANKID VISHING

- Brottsvinsterna har ökat med 87 % senaste året
- Genererar omkring 50 miljoner i brottsvinster/månad

Svensk Handel

The screenshot shows a text message conversation on a mobile phone. At the top, the contact is identified as 'Nordea'. The first message is a system-generated notification: 'under Logga in > Fler Tjänster Privat > Avtal och meddelanden.' Below this is a header 'Hälsningar Norde' and a button 'Visa alla' with a right-pointing arrow. The time '13:05' is shown on the right. A date separator indicates 'torsdag 4 november 2021'. The next message, from a contact with a purple profile icon, reads: 'Hej, vi misstänker bedräglig aktivitet på ditt konto. Vänligen ring spärrservice snarast på tel' followed by a redacted phone number. Below this is 'Referens:' followed by another redacted number. The message ends with 'Med vänlig hälsning Nordea' and the time '18:33'. The final message, also from the same contact, says: 'Hej, Vänligen ring handläggare' followed by a redacted name, 'för inbokat telefonmöte på tel'. A scroll-down arrow is visible at the bottom right of the message.

FÖREBYGGANDE ÅTGÄRDER

VAR UPPMÄRKSAM PÅ:

- Meddelanden från okända avsändare eller med konstigt innehåll från tillsynes kända avsändare
- Mejl som innehåller uppenbara stavfel eller grammatiska fel
- Mejl där visningsnamn och avsändaradress inte stämmer överens.
- Felmatchade e-postdomäner – Om mejlet påstås komma från ett seriöst företag, som Microsoft eller din bank, men skickas från en annan e-postdomän som Gmail.com eller microsoftsupport.ru är det förmodligen ett bedrägeri

VIKTIGT:

- Klicka aldrig på länkar och öppna aldrig filer i mejl från okända avsändare.
- Lämna aldrig ut koder, lösenord eller kontouppgifter till någon.
- Om någon ringer upp och du är osäker på uppringarens identitet, lägg på luren eller be att få ringa tillbaka på ett nummer du själv känner till.

VD-BEDRÄGERIER

- Bedragare tar kontakt med ekonomiansvarig på företaget
- Hävdar att det finns obetalda fakturor som skyndsamt måste betalas
- VD/högt uppsatt (falsk) chef tar kontakt för att styrka att fakturan är äkta

VD-BEDRÄGERI

Från: David Wang <david.wang@bmckenzie.net>

Skickat: den 13 september 2019 09:24

Till:

Ämne: Overdue Reimbursement

Good Morning Pernilla.

I was directed to reach out to you which is long overdue.

An invoice to this effect was issued as a matter of course. I would appreciate your advice.

I will be expecting your feedback.

Kind Regards.

David Wang.
Accounts Administrator & Senior
Baker & McKenzie LLP.
100 New Bridge St, London EC4A 3DF
United Kingdom.
E: david.wang@bmckenzie.net
P: +447441392519

**Baker
McKenzie.**

INVOICE

Baker & McKenzie Advokatbyrå

Vasagatan 7,
101 23 Stockholm,
Sweden.
Org number:916823-15051

BILL TO

QTY

1	Consultancy Services Arbitration.
---	--------------------------------------

Från: Jonas Hansson <ceo@magpiegroupdb.com>

Skickat: den 20 oktober 2020 13:34

Till: Caroline Nyholm <caroline@avestapark.se>

Ämne: Obetald faktura

Hej Pernilla

Jag mottog detta meddelande från Emelie Hager (en advokat från Baker Mckenzie) angående en sen räkning och jag bad honom att kontakta dig. Jag har också skickat honom ett mail nu.

Denna betalning avser ett framtida kontrakt i Stockholm som Baker McKenzie förhandlar på vår vägnar. Jag kommer att förse dig med detaljerna i denna händelse senare efter styrelsens granskning.

Jag förstår att fakturaen som skickades före slutade i vår spam. Kan vi betala denna faktura idag?

Vänliga hälsningar!!

Jonas Hansson

Litet L



nina.jelver@svenskhandel.se

nina.jelver@svenskhandel.se



Stort i

FÖREBYGGANDE ÅTGÄRDER

- Upprätta rutiner som innebär möjlighet att nå beslutsfattare för extra verifiering, vid betalningar över ett visst belopp, t ex att kunna motringa för godkännande mot en i förväg upprättad kontaktlista
- Var observant på avsändarens mailadress. Var även uppmärksam så att domänen stämmer överens med avsändarens mailadress; *.se* eller *.com*. Det förekommer rättstavat namn men att domänen är fel
- Upprätta rutiner för att kontrollera ändrade kontouppgifter från leverantörer – och då inte genom att maila tillbaka på samma adress som den uppgiften kom ifrån
- Var extra vaksam på e-post som är oväntad eller där uppgifter ska ändras mot vad det brukar vara

CYBERATTACKER

Nationella statsaktörer - geopolitiska

Cyberkriminella - tjäna pengar

Hacktivister - ideologiska

Terroristgrupper - ideologiska/våld

Spänningsökare - tillfredställelse



RANSOMWARE

- Skadlig kod som krypterar dina filer
- 623 miljoner ransomware-attacker under 2021
- 85 % inleds med phishing
- 30 % klickar vid phishing
- Lösensummorna som begärs blir allt högre
- "Ransomware as a service"



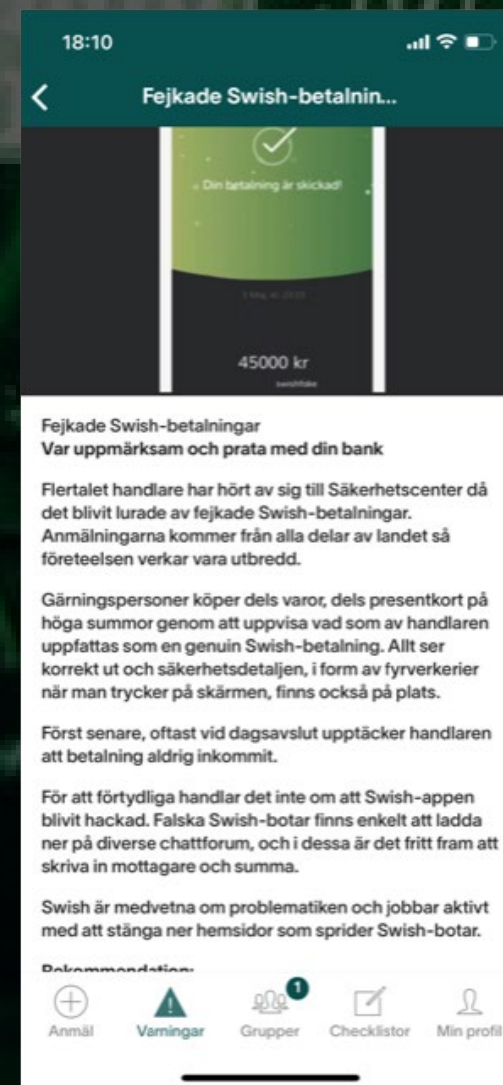
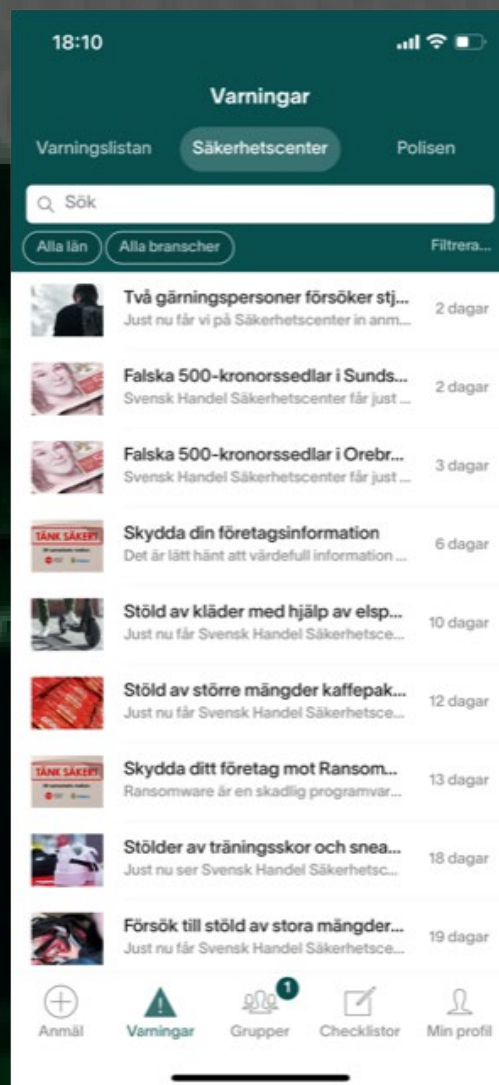
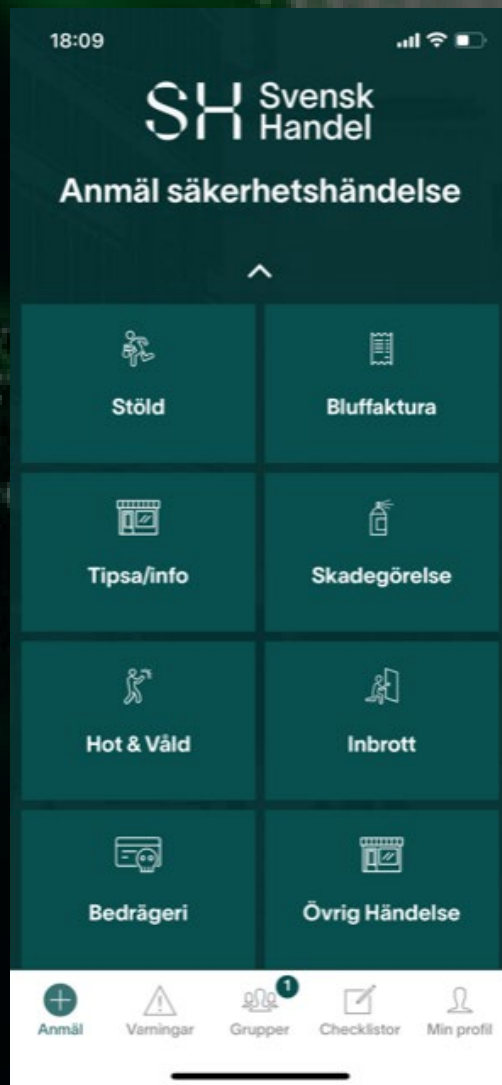
SÅ MINSKAR DU RISKEN ATT DRABBAS AV SKADLIG KOD – RANSOMWARE

- Om du inte har kompetensen internt, ta hjälp utifrån.
- Om du är ett mindre företag med begränsade möjligheter att anlita säkerhetskonsulter, nyttja de professionella aktörernas molntjänster
- Ha beredskap! Se över vilken information är mest värd att skydda och ta regelbundet säkerhetskopior på den information som du inte kan vara utan.
- Håll dina programvaror ständigt uppdaterade
- Aktivera flerfaktorsautentisering där det är möjligt.
- Installera brandvägg- och antivirusprogram
- Koppla aldrig in okända, externa enheter i din dator
- Klicka inte på bilagor, reklam och länkar om du är osäker på avsändaren
- Se över behörigheterna på företaget
- Utbilda din personal
- Säkra en alternativ kontaktväg

OM DU SKULLE DRABBAS, HÄR ÄR ÅTGÄRDERNA NÄR RANSOMWARE ÄR ETT FAKTUM

- Om du inte har kompetensen internt, ta hjälp utifrån direkt
- Polisanmäl händelsen i ett tidigt skede
- Försök att isolera de smittade enheterna
- Se till så att det genomförs en intern utredning – vad hände, hur kunde det hända?
- Säkerställ i er utredning att angreppet är åtgärdat och att angriparen inte har fortsatt tillgång till IT-miljön genom behörigheter och/eller skadlig kod i systemet
- Innan återställning av säkerhetskopior sker, kontrollera så att kopiorna inte också har drabbats
- Betala inte!
 - 80 % av de som betalar får inte tillbaka all information
 - 4 av 5 företag utsätts igen

Anmäl de brott ni drabbas av!





TACK!

Nina Jelver

nina.jelver@svenskhandel.se

010-47 18 516