SJU TIPS FÖR ATT FÖRHINDRA UTPRESSNINGS-PROGRAM

Skadlig programvara som använder kryptering för att kidnappa data har blivit mycket framgångsrik de senaste åren. Syftet med denna programvara är att pressa pengar från offren med löften om att återställa krypterade data.

Liksom andra datorvirus hittar den vanligen in till en enhet genom att utnyttja en säkerhetslucka i sårbar programvara, eller genom att lura någon att installera den. Sådana här utpressningsprogram ger sig på högprofilerade offer som sjukhus, skolor och polisavdelningar.

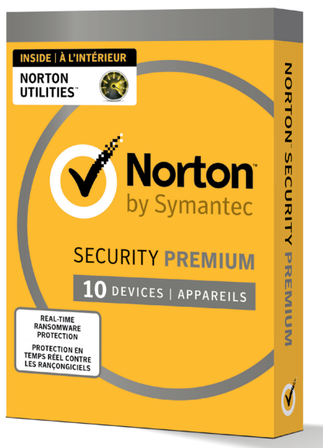
Nu har de tagit sig in i datorer i hemmet.

Det finns några saker du bör tänka på när det gäller utpressningsprogram.

Den ohederliga affärsmodellen med utpressningsprogram har visat sig vara en lukrativ bransch för brottslingar. Genom åren har dess dåliga rykte fått polisen att samarbeta med internationella myndigheter för att identifiera och få bort bluffoperatörer.

De flesta av angreppen med utpressningsprogram som har ägt rum tidigare har varit kopplade till bristfälliga skyddsmetoder.

1. ***BETALA INTE LÖSENSUMMAN.*** Det uppmuntrar bara angriparna och ökar deras resurser. Även om lösensumman betalas, är det ingen garanti att du får tillbaka åtkomst till dina filer.
2. ***ÅTERSTÄLL ALLA PÅVERKADE FILER FRÅN EN SÄKERHETSKOPIA DU LITAR PÅ.*** Återställning av filer från en säkerhetskopia är det snabbaste sättet att återfå åtkomsten till alla data.
3. ***LÄMNA INGEN PERSONLIG INFORMATION*** när du besvarar e-postmeddelanden, okända telefonsamtal, SMS-meddelanden eller snabbmeddelanden. Nätfiskare försöker lura anställda att installera malware, eller skaffa information för kommande angrepp genom att utge sig för att vara från IT. Kontakta IT-avdelningen direkt om du eller dina medarbetare får misstänkta samtal.
4. ***ANVÄND VÄLRENOMMERADE ANTIVIRUSPROGRAM OCH EN BRANDVÄGG.*** Det är ytterst viktigt att underhålla en stark brandvägg och att alltid hålla säkerhetsprogramvaran uppdaterad. Det är viktigt att använda antivirusprogram från ett välrenommerat företag eftersom det finns falsk programvara på marknaden.
5. ***ANVÄND INNEHÅLLSSÖKNING OCH FILTRERING PÅ DINA E-POST-SERVRAR.*** Inkommande e-post ska genomsökas efter kända hot och bör blockera alla typer av bifogade filer som kan utgöra ett hot.
6. ***SE TILL ATT ALLA SYSTEM OCH PROGRAM ÄR UPPDATERADE MED RELEVANTA KORRIGERINGAR.*** Utnyttjandepaket som finns på komprometterade webbplatser används vanligtvis för att sprida malware. Det är nödvändigt att regelbundet korrigera sårbarheter i program för att förhindra smitta.
7. ***OM DU RESER BÖR DU FÖRVARNA IT-AVDELNINGEN***, särskilt om du kommer att använda offentlig, trådlös internetanslutning. Se till att du använder ett pålitligt virtuellt privat nätverk (VPN) som Norton WiFi Privacy för åtkomst till offentliga Wi-Fi-nätverk.



Brottslingar som använder utpressningsprogram angriper ofta små och medelstora företag. Precis som andra internetangrepp är utpressningsprogram en brottslig verksamhet som enkelt kan undvikas med ovanstående lösningar. Norton Security Premium i kombination med utbildning i dessa hot är en utmärkt skyddsplan för dagens cyberlandskap.