

OUCH!

Det månatliga nyhetsbrevet om säkerhetsmedvetenhet till dig!

Shoppa säkert på nätet

Översikt

Det börjar närma sig jultider och snart kommer miljontals människor att leta efter de perfekta julklapparna. Många av oss kommer att handla på nätet för att hitta bra erbjudanden och för att undvika trängsel. Tyvärr kommer Cyberbrottslingar också vara aktiva med att skapa falska webbsidor och använda andra taktiker för att lura människor. I detta nyhetsbrev kommer vi att förklara hur du shoppar säkert på nätet och undviker att bli ett offer.

Falska nätbutiker

Cyberkriminella skapar falska nätbutiker som liknar de riktiga nätbutikerna eller använder samma namn som välkända butiker eller varumärken. När du söker efter de bästa onlineerbjudanden kan du hamna på en av dessa falska webbsidor. Om du köper från en sådan webbsida kan du få förfalskade eller stulna varor eller så kanske dina inköp aldrig levereras.

Skydda dig mot falska nätbutiker:



När det är möjligt, köp från kända nätbutiker som du har använt tidigare och litar på. Skapa bokmärken för nätbutiker som du har besökt och har förtroende för.



Se upp för priser som är betydligt bättre än de som finns i de etablerade nätbutikerna. Om ett erbjudande låter för bra för att vara sant är det troligen falskt.



Var misstänksam om webbsidan liknar den du använde tidigare, men webbsidans domännamn eller butikens namn är något annorlunda. Du brukar till exempel shoppa hos Amazon, vars webbadress är www.amazon.com, men handlar i stället på en falsk webbplats som har en liknande webbadress där bokstaven 'o' har ersatts med siffran "0".



Skriv namnet på nätbutiken eller dess webbadress i en sökmotor för att se vad andra har sagt om den. Leta efter termer som "bedrägeri", "bluff", "aldrig mer" eller "falskt."



Använd unika lösenord för dina onlinekonton. Kommer du inte ihåg dina lösenord? Överväg att lagra dem i en lösenordshanterare.

Bedragare på legitima webbplatser

Var på din vakt även när du handlar på betrodda webbplatser. Stora nätbutiker erbjuder ofta produkter som säljs av olika individer eller företag som kan ha bedrägliga avsikter. Sådana webbsidor är som riktiga marknader, där vissa säljare är mer pålitliga än andra. Kontrollera varje säljares rykte innan du gör en beställning. Var försiktig med säljare som är nya i nätbutiken eller som säljer föremål till ovanligt låga priser. Granska nätbutikens policy för köp från sådan tredje part. Om du är osäker, köp föremål som säljs av nätbutiken och inte av tredjepartsförsäljare som använder webbplatsen för att sälja sina föremål.

Betalningar online vid inköp

Kontrollera regelbundet dina kreditkortsuppgifter för att identifiera misstänkta avgifter. Om det är möjligt, aktivera att du får ett meddelande på e-post, sms eller app varje gång ditt kreditkort har använts. Ring och rapportera direkt ditt kreditkortsföretag om du upptäcker misstänkta transaktioner. Undvik att använda betalkort när det är möjligt. Betalkort tar pengar direkt från ditt bankkonto och vid ett bedrägeri kan du få mycket svårare att få tillbaka dina pengar. Ett annat alternativ är att använda välkända betaltjänster för köp online, till exempel PayPal eftersom du inte behöver lämna ut ditt kreditkortsnummer till säljaren. Slutligen överväg att använda presentkort för köp på nätet.

Bara för att en nätbutik har ett väl utformat och professionellt utseende betyder det inte att den är legitim. Om webbplatsen gör dig obekväma, använd inte den. Använd istället en välkänd webbplats som du kan lita på eller har använt tidigare.

Visolit är nordens ledande specialist på molntjänster. Visolit har för närvarande Europas största och mest moderna driftsplattform för SMB-marknaden. Vi levererar allt från komplett IT-drift till enklare IT-tjänster som anpassas och integreras utifrån kundens existerande behov och infrastruktur. Med våra tjänster får små och medelstora företag tillgång till IT med en kvalitet och säkerhet som normalt är undantaget stora internationella företag. www.visolit.se eller följ oss på LinkedIn <https://www.linkedin.com/company/visolit>

Gästredaktör

Lenny Zeltser är Chief Information Security Officer på Axonius och Senior Instruktor och författare på SANS Institut. Du kan följa honom på Twitter som [@lennyzeltser](https://twitter.com/@lennyzeltser) samt läsa hans blogg på zeltser.com.



Referenser

Social Engineering: <http://www.sans.org/u/X7k>
Scamming You Through Social Media: <http://www.sans.org/u/X7p>
Making Passwords Simple: <http://www.sans.org/u/Xu9>

OUCH! Publiceras av SANS Security Awareness och distribueras under [Creative Commons BY-NC-ND 4.0-licens](https://creativecommons.org/licenses/by-nc-nd/4.0/). Du kan fritt distribuera nyhetsbrevet eller använda det i ditt medvetenhetsprogram så länge du inte ändrar innehållet i nyhetsbrevet. För översättning eller mer information, vänligen kontakta www.sans.org/security-awareness/ouch-newsletter. Redaktion: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Översatt av: Johan Ahlberg