

OUCH!

Det månatliga nyhetsbrevet om säkerhetsmedvetenhet till dig!

Sök online efter dig själv

Översikt

Du har säkert redan hört hur viktigt det är att skydda din integritet och informationen du delar online. För att demonstrera detta ska vi försöka med något nytt, vi ska visa dig hur du kan göra research om dig själv och upptäcka vilken information som är allmänt känd om dig. Processen kallas för OSINT, det är ett tjsigt sätt att säga Open Source Intelligence. Detta betyder att forska i publika källor online för att se hur mycket information du kan inhämta om en dators IP adress, ett företag eller en person som dig själv. Kom ihåg att cyberbrottslingar också använder dessa verktyg och metoder. Ju mer en cyberbrottsling kan lära sig om dig ju bättre kan de skapa en riktad attack. Konceptet har funnits i flera år men de senaste verktygen har bidragit till att det är mycket enklare att uppnå en riktad attack.

Hur du hittar informationen

Du kommer inte hitta all information på en enda webbsida. Det du gör är att du börjar med en webbsida, lär dig några detaljer, därefter nyttjar du detaljerna du har lärt dig för att leta vidare på andra webbsidor. Därefter kombinerar och jämför du dina resultat för att skapa en profil över personen du kartlägger. Ett bra ställe att börja är med sökmotorer som Google, Bing eller DuckDuckGo. Dessa har indexerat olika information om dig, så börja din undersökning genom att söka med fler än en sökmotor. Börja med att skriva in ditt namn inom citattecken, därefter kan du utöka din sökning med något som kallas för operators. Operators är symboler eller text som kan bättre definiera vad du letar efter. Det är speciellt viktigt om du har ett vanligt namn, då kan det t.ex. behövas information som din e-postadress eller vilken stad du bor i. Lär dig gärna mer om hur du använder operatörer och avancerade söktekniker i referensmaterialet. Exempel kan inkludera:



- **“FirstName LastName” > vilken information kan jag hitta online om denna person.**
- **“FirstName LastName@” > hittar möjliga e-postadresser som är associerade med denna person.**
- **“FirstName lastName” filetype:doc > hittar worddokument som innehåller personens namn.**

Det finns också dedikerade webbsidor som samlar information om personer. Testa en av dessa sidor för att se vad som är allmänt känt om dig. Kom ihåg att dessa webbsidor inte alltid är träffsäkra och kan ha vissa beroenden till vilket land personen bor i. Du kan behöva söka på flera webbsidor för att verifiera den information som du hittar.



- <https://pipl.com>
- <https://cubib.com>
- <https://familytreenow.com>

Slutligen, det finns många andra webbsidor där du kan lära dig mer. T.ex. Google Images, Google Maps, Social Media, folkbokföring och mycket mer. För en interaktiv lista över olika webbsidor som du kan nyttja för att lära dig mer om dig själv rekommenderar vi ett besök hos OSINT Framework <https://osintframework.com>

Varför söka efter sig själv online?



1. Lär dig vad andra personer och organisationer har samlat, publicerat eller delat om dig online (ex kyrkor, skolan, sportklubbar eller andra organisationer).
2. Förstå att dessa tillgångar är tillgänglig för vem som helst, något som även inkluderar cyberbrottslingar som kan använda den informationen för att angripa dig. Ett skydd är att vara källkritisk. T.ex. om du tar emot ett brådskande telefonsamtal från någon som uppger sig ringa från din bank genom att de presenterar en del grundläggande information om dig bevisar inte att det faktiskt är din bank. Vid minsta misstanke avsluta samtalet artigt och ring till din bank på ett känt telefonnummer för att bekräfta att det är rätt. Samma sak gäller vid e-postmeddelanden, bara för att ett e-postmeddelande innehåller en del känd information om dig betyder inte att det är legitimt.
3. Överväg vilken information du delar publikt och vilken påverkan den informationen kan ha på dig, din familj eller din arbetsgivare.

TeleComputing är nordens ledande specialist på molntjänster. TeleComputing 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.telecomputing.se eller följ oss på LinkedIn <https://www.linkedin.com/company/telecomputing>

Gästskribent

Nico Dekens (@dutch_osintguy) är specialiserad inom OSINT. Han äter, sover och lever allt som handlar om insamling och analys av cyberunderrättelser. Nico föreläser internationellt om ämnen som OSINT, IoT och säkerhet hos Fortune 500 företag och regeringar.



Källor

- Social Engineering: <https://www.sans.org/u/LW6>
Top Tips for Social Media: <https://www.sans.org/u/LWb>
Search Engine Operators: <https://support.google.com/websearch/answer/2466433>
OSINT Framework: <https://osintframework.com/>
SANS OSINT Course SEC487: <https://www.sans.org/u/LWZ>

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: Erik Täfvander & Johan Ahlberg