Det Månatliga Nyhetsbrevet Om Säkerhetsmedvetenhet för Datoranvändare

OUCH!

I DENNA UTGÅVA…

- Social Manipulering
- Upptäcka / Stoppa Social Manipulering Attacker
- Förhindra framtida attacker

Social Manipulering

Översikt

En vanlig missuppfattning folk har om cyber angripare är att de bara använder avancerade hackerverktyg och tekniker för att bryta sig in i folks datorer, konton och mobila enheter. Detta är helt enkelt inte sant. Cyber angripare har lärt sig att ett av de enklaste sätten att stjäla information eller hacka din dator är genom att helt enkelt prata med och vilseleda dig. I detta nyhetsbrev kommer vi att lära oss hur dessa typer av mänskliga attacker, som kallas för social manipulering attacker, funkar och vad man kan göra för att skydda sig.

Gäst Redaktör

Alissa Torres är en certifierad SANS instruktör som specialiserat sig på avancerade dator kriminalteknik och incidenthantering. Hennes branscherfarenhet omfattar tjänstgöring med incidenthantering och arbete på ett internt säkerhetsteam som en digital rättsmedicinsk utredare. Alissa finns på Twitter som **@sibertor**.

Social Manipulering

Social manipulering är en typ av psykologisk attack där en angripare vilseleder dig till att göra något de vill att du ska göra. Social manipuleringskonst har funnits i tusentals år, tanken på att bluffa eller lura någon är inte ny. Men cyber angripare har lärt sig att denna teknik på nätet är oerhört effektiv och kan användas för att sikta in sig på miljontals människor. Det enklaste sättet att förstå hur social manipulering fungerar är att ta en titt på ett vanligt exempel från verkliga livet.

Du får ett telefonsamtal från någon som påstår sig vara från ett datorstödsföretag, din ISP eller kanske Microsoft tekniska support. Den som ringer berättar att de har märkt att datorn beter sig konstigt, som till exempel att den skannar Internet eller skickar spam, och de tror att den är infekterad. De har fått i uppdrag att utreda frågan och hjälper dig att skydda din dator. Sedan använder de olika tekniska termer och tar dig genom förvirrande steg för att övertyga dig om att din dator är infekterad.

Till exempel kan de be dig att kontrollera om du har vissa filer på datorn och gå igenom om hur man hittar dem. När du hittar dessa filer, kommer den som ringer försäkra dig om att dessa filer är ett tecken på att din dator är infekterad, när dessa filer i verkligheten är inget annat än vanliga systemfiler som finns på varje dator. När de har lurat dig att tro att din dator är infekterad, kommer de att pressa dig till att gå till en hemsida och köpa deras säkerhetsprogram eller be dig att ge dem fjärråtkomst till din dator så att de kan åtgärda det. Dock är programvaran som de säljer faktiskt ett skadligt program. Om du köper och installerar programvaran har de inte bara lurat dig att

© The SANS Institute 2014

Social Manipulering

infektera din dator, men du betalade dem att göra det. Om du ger dem fjärråtkomst till din dator för att fixa det, kommer de i själva verket att infektera den.

Kom ihåg att sociala manipulerings attacker som denna inte är begränsade till telefonsamtal; de kan hända med nästan all teknik, inklusive nätfiskeattacker via e-post, SMS, Facebook meddelanden, Twitter inlägg eller chatt. Det viktiga är att veta vad man ska se upp för.

Att lära sig att förebygga, upptäcka och stoppa social manipulering attacker är en av de mest effektiva åtgärder du kan vidta för att skydda dig.

Upptäcka / Stoppa Social Manipulering Attacker

Det enklaste sättet att försvara sig mot social manipulering attacker är att använda sunt förnuft. Om något verkar misstänkt eller inte känns rätt, kan det vara en attack. Några vanliga tecken på en social manipulering attack är:

- Någon skapar en enorm känsla av brådska. Om du känner att du är under press att göra ett mycket snabbt beslut, var misstänksam.
- Någon ber om information som de inte har tillgång till eller borde redan veta.
- Något är för bra för att vara sant. Ett vanligt exempel är att du får ett meddelande att du vann på lotto, även om du aldrig ens angett det.

Om du misstänker att någon försöker göra dig till ett offer för en social manipulering attack, kommunicera inte med personen längre. Om det är någon som ringer dig på telefon, lägga på. Om det är någon som chattar med dig online, avsluta anslutningen. Om det är en e-post som du inte litar på, ta bort den. Om attacken är arbetsrelaterade, se till att rapportera det till ditt support eller informationssäkerhetsgrupp direkt.

Förhindra Framtida Social Manipulering Attacker

Lyckligtvis finns det försiktighetsåtgärder man kan vidta för att förhindra att utsätta dig för framtida social manipulering attacker.

- **Dela Aldrig Lösenord**. Ingen organisation någonsin kommer att kontakta dig och fråga efter ditt lösenord. Om någon frågar dig om ditt lösenord, är det en attack.

- **Dela inte med dig för mycket**. Ju mer en angripare vet om dig, desto lättare är det för dem att hitta och vilseleda dig till att göra vad de vill. Även om du delar med dig små detaljer om dig själv kan detta med

Social Manipulering

tiden sättas samman för att skapa en fullständig bild av dig. Ju mindre du delar med dig offentligt, även på sociala medier, recensioner eller offentliga forum och mailinglistor, desto mindre troligt att du kommer att angripas.

- **Kontrollera kontakter**. Ibland kan du bli kontaktad av din bank, kreditkortsföretag, mobiloperatör eller andra organisationer av legitima skäl. Om du har några tvivel om huruvida en begäran om information är legitimt, be personen om deras namn och anknytningsnummer. Sedan hitta företagets telefonnummer från en betrodd källa, t.ex. numret på baksidan av ditt kreditkort, numret på ditt kontoutdrag, eller kanske numret på bolagets hemsida (se till att du skriver in webbadressen i din webbläsare själv). På detta sätt när du ringer organisationen, vet du att du verkligen pratar med dem. Även om det verkar som ett besvär, att skydda din identitet och personliga information är väl värt det extra steget.

LÄR DIG MER

Prenumerera på det månaltliga OUCH! nyhetsbrevet om säkerhetsmedvetenhet, ha tillgång till OUCH! arkiven, och lär dig mer om SANS lösningar inom säkerhetsmedvetenhet genom att besöka oss på http://www.securingthehuman.org

Swedish Version

OUCH! är översatt av Andreas Bohman och Marcus Andersson. Båda arbetar inom informationssäkerhetsbranchen och har många års erfarenhet i etablering av säkerhetsmedvetenhetsprogramm.

Resurser

E-post nätfiske:	http://www.securingthehuman.org/ouch/2013#february2013
Sociala nätverk säkerhet:	http://www.securingthehuman.org/ouch/2013#march2013
Undvik Bedrägerier:	http://www.onguardonline.gov/topics/avoid-scams

OUCH! utgivs av SANS Securing the Human och är distribuerat under Creative Commons BY-NC-ND 4.0 licens.
Du kan fritt distrubera nyhetsbrevet eller andvända det i ditt interna medvetenhetsprogramm så länge du inte ändrar nyhetsbrevet.

För översättning eller mer information, vänligen kontakta ouch@securingthehuman.org.
Redaktion: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Översatt Av: Andreas Bohman och Marcus Andersson

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus