OUCH! | February, 2015

Det Månatliga Nyhetsbrevet Om Säkerhetsmedvetenhet för Datoranvändare

OUCH!

I DENNA UTGÅVA…

Var Säker När du Reser

Översikt

I detta nyhetsbrev kommer vi att täcka hur du säkert kan ansluta till Internet och få saker gjorda när du reser.

Gäst Redaktör

Steve Armstrong är teknisk direktör för CyberCPR på Logically Secure, en certifierad SANS instruktör och tidigare kurs författaren på SANS. Han är aktiv på Twitter som **@Nebulator** och på Google plus: **+ SteveArmstrongSecurity**.

Innan du åker

Medan ditt nätverk hemma eller på jobbet kan vara säker, när du reser bör du alltid utgå från att alla nätverk som du ansluter till är opålitliga. Du vet aldrig vem är på det och vilka hot de kan utgöra. Några enkla pre-rese åtgärder kan gå en lång väg att skydda dina data medan du reser. En eller två veckor före resan:

- Identifiera vilka data du inte behöver på vilka enheter du tar med dig och sedan ta bort alla onödiga uppgifter. Detta kan avsevärt bidra till att minska effekterna om dina enheter är förlorade, stulna eller i beslag av tullen eller gränssäkerhetspersonal. Om din resa är relaterat av ditt arbete fråga din handledare om din organisation ger alternativa enheter som används specifikt för att arbeta under resan.
- För internationella resor, kolla vilken typ av eluttag landet använder, du kan behöva få en adapter för laddning av dina enheter. Dessutom, kolla vilken serviceplan du har för din telefon med din mobiloperatör. Ofta begär tjänsteleverantörer höga priser för internationell dataanvändning och du kanske vill inaktivera dina cellulära datakapacitet under resan eller ändra din serviceplan för internationella resor.
- Installera programvara på din enhet så att du kan spåra var din enhet är, och till och med radera den, om den är förlorad eller stulen. Många mobila enheter har redan denna funktion inbyggd och du kanske bara behöver aktivera det (kom ihåg att dessa behöver tillgång till Internet för att fungera).

En eller två dagar innan resan:

- Uppdatera din enheter, applikationer och antivirusprogram så att du kör den senaste versionen.
- Aktivera alla lämpliga säkerhetsinställningar på enheten, t.ex. dina brandväggar.
- Lås alla dina mobila enheter med ett starkt lösenord eller kod. På detta sätt, om du förlorar din enhet eller

Var Säker När du Reser

har det stulits, kan inte människor få tillgång till information på enheten.

- Kryptera alla dina enheter så att om de är förlorade eller stulna, kan inte datan nås. Vissa enheter såsom iPhone gör detta automatiskt om du ställer in ett lösenord eller en kod på enheten.
- Gör en fullständig säkerhetskopia av alla dina enheter. På detta sätt, om något händer med dem när du reser, har du fortfarande alla dina data på ett säkert ställe.

Nyckeln till att vara säker medan du reser är att säkra dina enheter innan de lämnar hemmet, hålla dem under uppsikt och veta var de är hela tiden, och kryptera alla aktiviteter på nätet.

Förlorade / stulna enheter

När du börjar resa var noga med den fysiska säkerheten för dina enheter. Till exempel, lämna aldrig dina enheter i bilen där folk lätt kan se dem, eftersom brottslingar kommer helt enkelt att krossa bilens fönster och ta allt av värde de kan se. En idé är att ta med ett kabellås så att du kan fysiskt låsa dina enheter, till exempel din bärbara dator, när du lämnar dem. Medan brottsligheten är definitivt en risk, vad du kanske inte inser är att det är faktiskt mycket mer troligt att du förlorar din enhet. Enligt en tio års undersökning av Verizon, är det 15 gånger mer sannolikat att man förlorar en enhet än att få den bestulen. Detta innebär att du bör alltid dubbelkolla att du fortfarande har dina enheter när du reser, till exempel när när du går igenom säkerhetenkontrollen på flygplatsen, lämnar en taxi eller restaurang, checkar ut från ett hotellrum eller innan du stiger av ditt flygplan.

Wi-Fi

Åtkomst till Internet när du reser innebär ofta att använda offentliga Wi-Fi-åtkomstpunkter, såsom de du hittar på ett hotell, ditt lokala kafé, eller flygplatsen. Problemet med offentliga Wi-Fi-åtkomstpunkter är inte bara att du är aldrig säker på vem som installerade dem, men man vet aldrig vem som är ansluten till dem. Som sådana bör de betraktas som opålitliga och det är faktiskt därför du tog alla steg för att säkra dina enheter innan du reste. Dessutom använder Wi-Fi radiovågor för att kommunicera från din enhet till den trådlösa åtkomstpunkten. Detta innebär att någon som är fysiskt nära dig kan potentiellt avlyssna och övervaka dessa meddelanden.

Det är därför om du använder Wi-Fi, du måste se till att all din online aktivitet är krypterad. Till exempel, när du ansluter online med din webbläsare se till de webbplatser du besöker krypteras (de kommer att ha “https: //” i adressen och en bild av ett sluten hänglås). Dessutom kan du ha vad som kallas ett VPN (Virtual Private Network) konto som kommer

Var Säker När du Reser

att kryptera alla dina aktiviteter online. Detta kan utfärdas till dig av jobbet, eller så kan du köpa VPN-funktioner för eget bruk. Om du är orolig för att det inte finns några Wi-Fi-åtkomstpunkter som du kan lita på, överväg att uppbinda till din smartphone. (Varning: Som vi nämnde tidigare, kan detta bli dyrt när du reser utomlands, kontrollera med din operatör först).

Offentliga Resurser

Använd inte några offentliga datorer, till exempel datorer i hotellreceptioner, bibliotek eller internetkaféer. Du har ingen aning om vem har använt den datorn innan du och kan de ha smittat den offentliga datorn av misstag eller avsiktligt. Använd om möjligt bara enheter du har kontroll och förtroende över för all aktivitet online. Om du måste använda en offentlig dator, använd inte någon tjänst som kräver att du loggar in eller skriv ett lösenord.

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

Lösenord:	http://www.securingthehuman.org/ouch/2013#may2013
Tvåstegsverifiering:	http://www.securingthehuman.org/ouch/2013#august2013
Kryptering:	http://www.securingthehuman.org/ouch/2014#august2014
Säkra din nya Tablet:	http://www.securingthehuman.org/ouch/2013#december2013
Verizon DBIR 2014:	http://www.verizonenterprise.com/DBIR/2014/

Redaktion: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Översatt Av: Andreas Bohman och Marcus Andersson