Delmoment 5, frågor och svar.

1. Vilka två färgkombinationer är problematiska att läsa för de som har färgblindhet eller dyslexi?

* Färgblindhet innebär att man har svårt att skilja vissa färger från varandra, färgblindhet är medfött och ärftligt. Man kan också ha svårt att se skillnad på vissa färger. Den vanligaste formen gör att det är svårt att se skillnad på grönt och rött.

Det finns olika typer av färgblindhet så som:

* Röd-grön färgblindhet
* Gul-blå färgblindhet
* Total färgblindhet

Den färgblindhet som gör att en person inte ser några färger alls utan ser världen i en gråskala är mycket ovanligt.

Den vanligaste blindheten är mellan rött och grönt, alltså färger som har grönt eller rött i sig. Exempelvis så kan du ha svårt att se lila och blått då lila är en blandning mellan blått och rött. Man kan också ha svårt att se skillnad på grönt och brunt då brun är en blandning av grönt och rött.

Att ha röd-grön blindhet innebär inte att du ser gräsmattan röd eller stopp signalen grön. Utan det innebär att man har svårt att se skillnaden på rött och grönt.

Personer med dyslexi har lättare att läsa om kontrasterna inte är för skarpa. Svart färg mot vitt blir tröttande och har förklarats med att minnesbilden av ett ord inte försvinner tillräckligt snabbt när man flyttar till nästa ord. Det blir alltså en dubbelbild som är distraherande för personen. Om det är en svag toning på bakgrunden så blir det mer underlättande för de personer med dyslexi eftersom ”bilden” inte blir lika dominant.

1. Vad betyder följande: phishing, whitelist och blacklist?

* Phishing även kallat nätfiske är de vanligaste attack metoderna bland cyberkriminella idag. Metoden går ut på att via e-post, sms eller chatt tjänster lura mottagaren att öppna ett dokument, besöka en webbplats eller ladda ner en fil. Målet är att infektera enheten med skadlig kod eller också komma över personliga behörigheter som ett första steg i ett mer omfattande angrepp.

I grund och botten är nätfiske en form av en identitetsstöld där angriparen utger sig för att vara någon annan som exempel en myndighet, arbetsgivare eller ett företag. Attacken verkställs sedan genom att skicka falska meddelanden som uppmanar mottagaren att klicka på länkar eller sms i syfte om att få till sig känslig information eller infektera mottagarens enhet med skadlig kod.

Vanligt nätfiske skickas i många fall till stora grupper av mottagare utan större träffsäkerhet. Många cyperkriminella jobbar aktivt för att maximera lönsamheten i sin verksamhet, de har allt mer förfinade varianter av phishing såsom spear-phising och smishing.

Spear-phishing attacker riktar in sig mer på utvalda individer istället för slumpmässiga grupper. I dessa fall gör angriparen ett ordentligt förarbete som bland annat kan innefatta kartläggning av ett företags anställdas intressen i sociala medier mm.

Smishing förekommer också på sms, namnet kommer från phishing och sms. Attacken går ut på att angriparen skickar sms från en falsk avsändare i syfte om att få mottagaren att klicka på en länk som antingen installerar en skadlig kod eller förmår mottagaren att lämna ifrån sig känslig information.

Whitelist (vitlista) är en lista över objekt som får åtkomst till ett visst system eller protokoll. När en vitlista används nekas alla enheter åtkomst utom de som ingår i vitlistan. Exempel på olika vitlistapplikationer:

Är exempelvis en programmerare som använder vitlistor i program för att säkerhetskälla att endas vissa objekt ändras.

Eller några e system kan konfigureras för att endast acceptera meddelanden från e-postadresser som har lagts till av en användares vitlista.

Vitlistor är bra alternativ när endast ett begränsat antal enheter behöver åtkomst. Motsvarighet till whitelist är blacklist (svartlista). Blacklist är förteckning över identiteter som namn, adresser osv som nekas åtkomst till en eller flera tjänster. Exempelvis kan en e-postserver använda blacklist för kända avsändare av spam som nekas att skicka brev till servern.

Man kan använda detta även inom datasäkerhet där en blacklist används för att ta bort olämpliga tecken som exempel i html element för att undvika säkerhetsproblem. Det anses dock att vitlistor är att fördra för just detta.

Blacklist(svartlista) i sig som ord används för att utestänga, svartlista någon/något.

1. Sök på internet och ta reda på vad GDPR (som tidigare hette personuppgiftslagen) handlar om. Varför finns GDPR? Fundera även på hur det påverkar en person som arbetar med webbsidor. Skriv ett utförligt svar och tänk på att granska källan till informationen du hittar.

* Den 25 maj 2018 trädde ett nytt regelverk kring persondataskydd och dataskyddsförordning som heter GDPR (General Data Protection Regulation) i kraft efter ett beslut i EU. Regelverket ersatte personuppgiftslagen (PUL) och delvis patientlagen (PDL). GDPR innebär hårdare krav på hantering av personuppgifter. Alla verksamheter måste följa dataskyddsreglerna vid behandling av personuppgifter, det innebär bland annat att man måste följa de grundläggande principerna att se till att behandling av uppgifter har en rättslig grund och informera de registrerande om hur den organisation hanterar människors personuppgifter. Mycket handlar om att göra det tydligt för kunden vilken information som sparas, hur det sparas och vad som sker om deras uppgifter skulle komma på villovägar genom exempelvis en cyperattack. De företag eller organisationer som inte efterlever GDPR riskerar stora böter upp till 4 % av den årliga globala omsättningen eller 20 miljoner euro, beroende på vilken av summorna som blir störst. Det gäller oavsett om det är en offentlig myndighet, privat företag, en förening eller någon annan typ av verksamhet. Dataskyddsreglerna grundar sig i de mänskliga rättigheterna. Alla människor har rätt till respekt för privat och familjeliv och till skydd för sina personuppgifter.

Ett av syftena med dataskyddsförordningen är att skydda enskildas grundläggande rättigheter och friheter särskilt deras rätt till skydd av personuppgifter. Rätten till sitt privatliv uttrycks i den Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR= Europakonventionen). I EKMR ges en rätt till respekt för privat och familjeliv, hem och korrespons. Konventionen har nu införts som lag i Sverige.

Ett av några syften med denna dataskyddsförordning är att modernisera dataskyddsdirektivets regler från 1995 och att anpassa dem till det nya digitala samhälle. Genom GDPR hoppas lagstiftarna att kunna hjälpa näringslivet till en bättre kommunikation kring personuppgifter med sina konsumenter vilket på lång sikt kommer att öka tillväxten genom att fler personer litar på företagen som samlar informationen. Ett företag är personuppgiftansvarig för behandlingen av personuppgifter om sina anställda, kunder och leverantörer. Medan en myndighet är personuppgiftsansvarig för behandlingen av uppgifter om personer som förekommer i ärenden hos myndigheten.

För en person som jobbar med webbsidor så gäller GDPR att man gör så hög säkerhet som möjligt på sin hemsida så att besökarens personuppgifter inte läcker ut till obehörig part. Hemsidan ska även skydda besökarnas integritet genom att erbjuda dem möjlighet att kunna stänga av all osynlig spårning av hur de rör sig på din hemsida. De flesta hemsidor har en kod som försöker dölja och förstå hur användaren surfar och vilken typ av innehåll de söker.

Den personen som äger ett företag, organisation och hemsidan är ansvariga för att både företaget och att hemsidan följer GDPR lagen.

Om man jobbar med hemsidor så är det relativt enkelt att fixa så hemsidan följer GDPR lagen annars finns det webbyråer som kan tipsa eller hjälpa till.

En vanlig företagshemsida behöver följa fyra regler för att klassas som korrekt och GDPR säker.

* Hemsidan behöver ha ett SSL certifikat. Om hemsidan inte har SSL certifikat så innebär det att det är högre risk för att dina besökare får sin data stulen.
* Om man har ett kontaktformulär på sin hemsida så måste man ha en integritetspolicy på sidan.
* Om man använder sig av cookies så måste du även ha en tydlig cookie ”knapp” som ger dina besökare valet att låta dina cookies spåra dem när de befinner sig på hemsidan eller inte. Det kallas för en opt-out.

Sedan om du ansvarar för en statlig eller en kommunal hemsida så måste man även följa regler som gör att hemsida är användarvänlig för de som har någon form av funktionsnedsättning som exempelvis blindhet eller mental nedsättning. Detta är inte ett måste för privata företag enligt lagen.

Det finns lite olika saker man kan göra för att säkra GDPR på sin hemsida. Som att ha ett SSL certifikat som har nämnt tidigare, som passar ens hemsida eftersom att GDPR lagen kräver att känslig och personlig information/data ska skyddas så vill man att sådan information på nätet ska krypteras. Och det gör man med ett SSL certifikat, certifikatet gör att informationen är säker när den transporteras mellan avsändare och mottagare som ex webbläsare och webbserver. SSL bevisar att själva bakomliggande tekniken för att säkra kommunikationen mellan webbläsaren och webbservern är av högsta kvalitet. Det behövs för att överföra informationen ”säkert” så att det inte längre står ”osäkert” på hemsidan. SSL certifikat fungerar som ett intyg för att legitimera en part i kommunikationen. Har man en webbshop så behöver man köpa en dyrare SSL certifikat.

Om man har cookies på sin hemsida så måste man lägga till en ”cookie policy” på hemsidan. Cookies är den kod som google motorn lägger till för att man ska få riktade annonser som passar ens surf mönster. Besökaren på sidan måste ha valmöjligheten att välja bort detta om den vill med en ja/nej knapp. Att kunna stänga av spårningen om den vill helt enkelt.

Skrivet av Ida Casperson