Namn på arbetet

Komvuxarbete



Robin Roxenrot

Hermods 2025

Per-Arne Bystedt

ABSTRACT

INNEHÅLLSFÖRTECKNING

1. INLEDNING

1.1 Introduktion

1.2 Syfte

1.3 Teori

1.4 Frågeställningar

1.5 Avgränsningar

1. METOD

2.1 Material

2.2 Utförande

1. RESULTAT

3.1 Frågeställning 1

3.2 Frågeställning 2

3.3 Frågeställning 3

1. METODDISKUSSION
2. DISKUSSION OCH SLUTSATS

5.1 Diskussion

5.2 Slutsatser

1. KÄLLFÖRTECKNING OCH KÄLLKRITIK

6.1 Källförteckning

6.2 Källkritik

1. BILAGOR

7.1 Bilaga 1

7.2 Bilaga 2

INLEDNING

* 1. Introduktion:

Den snabba digitaliseringen har lett till att cybersäkerhet blivit en av de mest kritiska frågorna för både individer och organisationer. Med ökande cyberhot, såsom dataintrång, ransomware-attacker och identitetsstölder, är det nödvändigt att förstå vilka säkerhetsåtgärder som är mest effektiva för att skydda känslig information. I takt med att samhället blir alltmer beroende av digitala tjänster har även lagstiftning och säkerhetsprotokoll utvecklats för att möta dessa hot.

Tidigare forskning och rapporter har visat att många cyberattacker beror på bristfällig säkerhetsmedvetenhet, svaga lösenord och sårbara system¹. Genom detta arbete undersöks hur cybersäkerhet kan förbättras genom tekniska lösningar och ökad medvetenhet hos användare.

* 1. Syfte: Syftet med denna studie är att analysera och förstå cybersäkerhetens betydelse för både privatpersoner och organisationer. Arbetet fokuserar på vilka hot som är vanligast, vilka säkerhetsåtgärder som kan implementeras och hur cybersäkerhetsmedvetenhet kan förbättras.
  2. Teori: Cybersäkerhet bygger på flera grundläggande principer och metoder för att skydda information och digitala system från hot och attacker. En av de mest centrala modellerna inom området är **CIA-triaden (Confidentiality, Integrity, Availability)**, som används för att säkerställa att information förblir konfidentiell, oförändrad och tillgänglig vid behov¹.

En annan viktig referensram är NIST:s ramverk för cybersäkerhet, vilket erbjuder riktlinjer för hur organisationer kan identifiera, skydda, upptäcka, reagera på och återhämta sig från cyberhot². Dessa principer används ofta i både privata och offentliga verksamheter för att stärka IT-säkerheten och minska riskerna för dataintrång.

Forskning inom cybersäkerhet har också visat att en kombination av tekniska lösningar och mänskliga faktorer är avgörande för ett effektivt skydd³. Social ingenjörskonst, där angripare manipulerar användare till att avslöja känslig information, är en av de största säkerhetsriskerna. Därför är säkerhetsmedvetenhet och utbildning av användare lika viktiga som tekniska försvarsåtgärder, såsom kryptering och flerfaktorsautentisering.

* 1. Avgränsningar: Här ska du förklara vad du inte kommer att ta med i din undersökning. Du behöver avgränsa dig för att inte undersökningen ska svälla ut och bli svår att överblicka.

METOD

2.1 Materiel: Räkna upp den utrustning du använde.

2.2 Utförande: Beskriv hur du gick till väga för att genomföra din undersökning. Någon annan person ska kunna upprepa undersökningen genom att följa din beskrivning.

Om du gör en litteraturstudie förklarar du det här.

RESULTAT

Här svarar du på dina frågeställningar. Gör om dem till påståenden istället för frågor.

METODDISKUSSIONEN

Här ska du resonera kring den metod du har använt för att få svar på dina frågeställningar. När man söker svar på frågeställningar finns det ofta olika metoder man kan använda. Du har använt *en* metod. Under den här rubriken ska du diskutera för- och nackdelar med just den metoden. Vilka svagheter finns? Vad är bra med metoden? Om du har gjort en praktisk undersökning ska du ta upp och resonera kring felkällorna här.

DISKUSSION OCH SLUTSATS

5.1 Diskussion: Här ska du analysera och resonera kring resultatet av undersökningen. Använd de vetenskapliga teorierna i dina resonemang.

5.2 Slutsatser: Här sammanfattar du diskussionen kring resultatet.

KÄLLFÖRTECKNING OCH KÄLLKRITIK

6.1 Källförteckning: Här ska du göra en förteckning över källor du använt. Använd Harvardsystemet.

6.2 Källkritik: Här ska du förklara *varför* du anser att källorna är trovärdiga.

BILAGOR

Om du har mycket data, bilder etc. kan de läggas in här istället för under ”Resultat”. Du hänvisar i så fall till de olika bilagorna i ditt resultat.