Provkonstruktion

Årskurs: Gymnasiet

Ämne eller kurs: Datorteknik 1a

Tema: Säkerhet och skydd av information

Syfte

Syftet med provet är att bedöma elevernas kunskaper om datasäkerhet, inklusive vanliga hot och skyddsåtgärder, samt att ge dem möjlighet att beskriva och analysera aspekter av datasäkerhet i en verklig kontext.

Koppling till styrdokument

Centralt innehåll

Målet för provet är att pröva elevers kunskap om datasäkerhet och skydd av information genom att återge följande centrala innehåll: “Vi kommer att gå igenom olika typer av hot samt strategier och teknologier som används för att skydda data, inklusive brandväggar, antivirusprogram och kryptering.”

Kunskapskrav

Provet omfattar följande kunskapskrav: “Eleven ska kunna beskriva och ge exempel på vanliga säkerhetshot mot datorsystem och kunna redogöra för olika skyddsmekanismer och strategier för att hantera dessa hot.”

Prov

Faktafrågor

1. Vad innebär datasäkerhet?
A) Att använda kraftfulla datorer
B) Att skydda information från obehörig åtkomst
C) Att skapa användarkonton
D) Att installera spelprogram

2. Vilket av följande är en typ av skadlig kod?
A) Brandvägg
B) Antivirusprogram
C) Virus

D) Kryptering

3. Vad syftar phishing på?
A) Att förbättra nätverksprestanda
B) Att lura användare att avslöja känslig information
C) Att installera säkerhetsuppdateringar
D) Att övervaka nätverkstrafik

4. Vilken av följande åtgärder kan bidra till att förbättra datasäkerheten?
A) Använda starka lösenord
B) Låsa datorn när den inte används och inte logga ut
C) Dela hårdvara med andra användare
D) Hålla programvara utdaterad

5. Vilket av följande är ett exempel på en skyddsmekanism?
A) DDoS-attack
B) Brandvägg
C) Malware
D) Phishing

6. Vad är en DDoS-attack?
A) En metod för datakryptering
B) En typ av antivirusprogram
C) En attack där många enheter överbelastar ett system
D) En strategi för att hantera information

7. Vilken typ av hot kan uppstå genom social ingenjörskonst?
A) Virus
B) Bedrägerier där människor luras att ge bort information
C) Brandväggar
D) Antivirusprogram

8. Vad kontrollerar en brandvägg?
A) Inkommande och utgående nätverkstrafik
B) Användarnamn och lösenord
C) Datorprogram
D) Filöverföringar

9. Vilken av dessa är en konsekvens av säkerhetsbrister?
A) Ökad webbläsart hastighet

B) Förlust av känslig information
C) Förbättrad tjänstefunktionalitet
D) Förbättrad användarupplevelse

10. Hur kan användare stärka sin egen datasäkerhet?
A) Genom att undvika att installera säkerhetsuppdateringar
B) Genom att hålla programvara och operativsystem uppdaterade
C) Genom att använda samma lösenord överallt
D) Genom att dela sina inloggningsuppgifter med andra

11. Vilket av följande är en vanlig typ av malware?
A) Trojan
B) Brandvägg
C) Kryptering
D) Antivirusprogram

12. Vad är syftet med kryptering?
A) Att öka dators hastighet
B) Att skapa en säkerhetskopiering
C) Att skydda data genom att göra den oläslig för obehöriga
D) Att organisera filer

13. Vilken roll har säkerhetsuppdateringar?
A) De hindrar datorn från att starta
B) De förbättrar användarens upplevelse
C) De åtgärdar säkerhetsbrister och sårbarheter
D) De ökar systemets hastighet

14. Vilken typ av information skyddar datasäkerhet?
A) Endast finansiell information
B) Endast personlig information
C) Både personlig och organisatorisk information
D) Endast företagsinformation

15. Vilka enheter kan vara måltavlor för datasäkerhetshot?
A) Alla datorer och mobila enheter
B) Endast stationära datorer
C) Endast servrar
D) Endast bärbara datorer

Resonerande frågor

1. Resonera kring vikten av datasäkerhet i dagens digitala samhälle.
Syftet är att ge eleverna möjlighet att reflektera över och analysera hur datasäkerhet påverkar individers och organisationers arbete.

2. Diskutera de mest effektiva skyddsmekanismerna mot malware och andra hot.
Genom att diskutera skyddsmekanismer får eleverna möjlighet att visa djup förståelse och kritiskt tänkande kring ämnet.

3. Analysera hur en fiktiv organisation kan stärka sin datasäkerhet med hjälp av de tekniker som lärts ut.
Här ges elever möjlighet att applicera sin kunskap praktiskt på en given situation, vilket demonstrerar deras förståelse av teorin i praktiken.

4. Reflektera över de potentiella konsekvenserna av ett dataintrång för en organisation.
Denna fråga uppmanar elever att tänka kritiskt omkring konsekvenserna av bristande datasäkerhet och att analysera risker.

5. Diskutera hur social ingenjörskonst kan påverka datasäkerheten och ge exempel på hur individer kan skydda sig.
Genom att diskutera social ingenjörskonst kan eleverna identifiera och förstå mänskliga faktorer i datasäkerhetsfrågor.

6. Resonera kring de etiska aspekterna av datasäkerhet och integritet.
Detta ger elever möjlighet att reflektera över samspelet mellan säkerhet och personlig integritet.

7. Analysera skillnaderna mellan olika typer av antiviruslösningar och vilken typ som skulle vara mest effektiv för en småföretagare.
Genom att analysera olika lösningar uppvisar eleverna sin förmåga att beakta specifika behov och krav inom datasäkerhet.

8. Reflektera över hur lagar och förordningar kring datasäkerhet kan påverka företag och organisationer.
Denna fråga ger elever möjlighet att koppla teori till verkligheten och förstå det juridiska perspektivet av datasäkerhet.

Bedömning

Provets poängfördelning är som följer:

Faktafrågor: 1 poäng per fråga, totalt 15 poäng. Resonerande frågor: 3 poäng vardera, totalt 24 poäng. För att uppnå följande betyg krävs:

För betyg E: Minst 8 poäng totalt.

För betyg C: Minst 12 poäng totalt (varav minst 3 poäng från resonerande frågor).

För betyg A: Minst 18 poäng totalt (varav minst 5 poäng från resonerande frågor).

Tags: Datorteknik 1a, Gymnasiet