Cybersecurity Academy

# Är du säker?

Cybersäkerhet i elevernas vardag – kunskap som gör skillnad

## Arbetsblad och filmlänkar – Högstadiet

# Filmlänkar

Filmerna Ditt digitala fotavtryck, Klicka smart och Digital rustning finns på svenska och lättsvenska, med undertexter på engelska, arabiska, tigrinska och somaliska. I presentationerna ligger filmerna på svenska med svensk undertext som standard. Via länkarna nedan kommer du till spellistorna på YouTube där samtliga versioner finns samlade.

## Lektion 1

**Tänk säkert**
https://youtu.be/K4FqzSqrjwE

**Ditt digitala fotavtryck**
https://www.youtube.com/playlist?list=PLIk39hnHx0Lv0ayyDRa50Z2tDGdne_b9e

## Lektion 2

**Klicka smart**
https://www.youtube.com/playlist?list=PLIk39hnHx0LsV2uVCgmBYzEx-3TMf__gP

**MrBeast**
https://x.com/MrBeast/status/1709046466629554577

## Lektion 3

**Digital rustning**
https://www.youtube.com/playlist?list=PLIk39hnHx0Lt-DBDkAmPB3x6Jl4iJaf22

# Arbetsblad: Bluffdetektiv (1)

Från: skolledning123@gmail.com

Ämne: BESTÄLL INNAN SKOLSTART

Hej elev!

Nu är det start på en ny termin och ni behöver klicka på denna länk för att beställa idrottskläder. ALLA SKA HA! Du vill inte vara den enda som inte har.

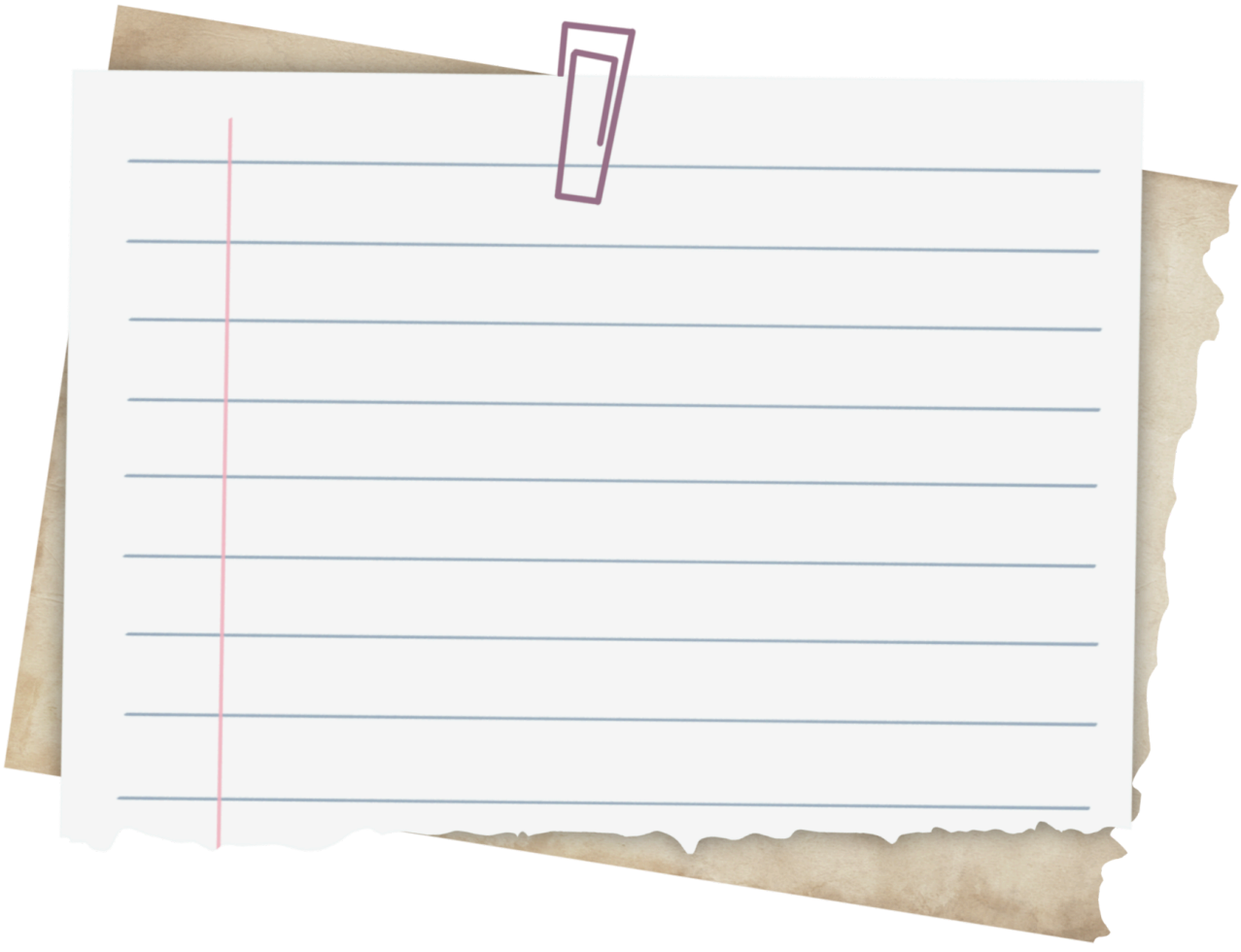
Det är JÄTTEVIKTIGT att alla beställer innan skolstart.

Länken är bara aktiv fram till skolstart. Beställ i tid och vinn ett pris!

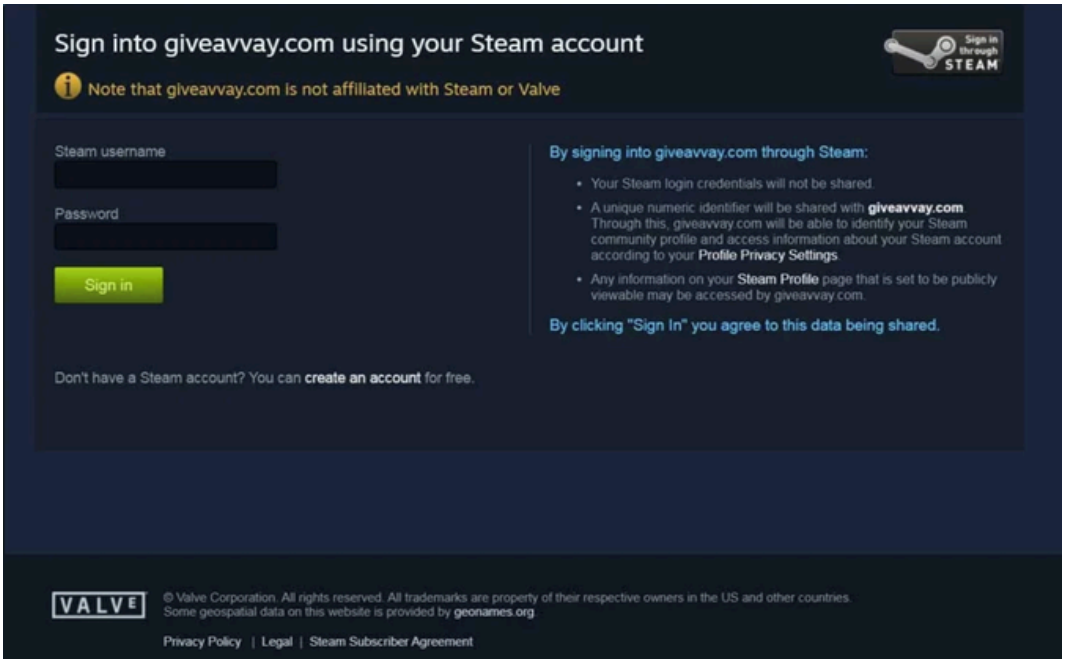
Med vänliga hälsningar,

Skolledningen

- Finns det något som känns konstigt eller misstänkt med meddelandet eller erbjudandet? Om ja, vilka varningssignaler kan ni hitta?
- Vad tror ni kan hända om man klickar på länken eller lämnar ut uppgifter?



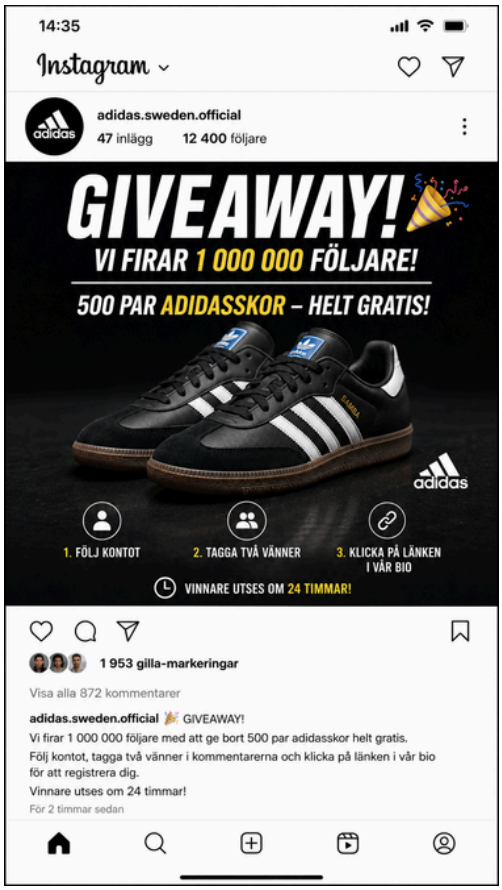
# Arbetsblad: Bluffdetektiv (2)



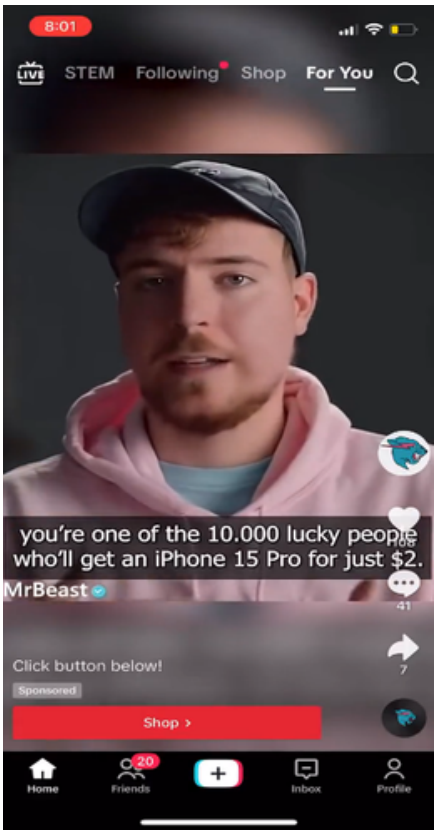

- Finns det något som känns konstigt eller misstänkt med meddelandet eller erbjudandet? Om ja, vilka varningssignaler kan ni hitta?
- Vad tror ni kan hända om man klickar på länken eller lämnar ut uppgifter?

# Arbetsblad: Bluffdetektiv (3)

- Finns det något som känns konstigt eller misstänkt med meddelandet eller erbjudandet? Om ja, vilka varningssignaler kan ni hitta?
- Vad tror ni kan hända om man klickar på länken eller lämnar ut uppgifter?



# Arbetsblad: Bluffdetektiv (4)




Skanna QR-koden för att se videon.
**Obs!** Visste du att även QR-koder kan vara luriga? Bedragare kan gömma skumma länkar bakom dem. Kolla alltid vart länken leder innan du klickar vidare – det brukar synas på skärmen när du skannat koden. Den här QR-koden ska ta dig till:
https://x.com/MrBeast/status/1709046466629554577
Stämmer det? Då är det OK att surfa vidare!

- Finns det något som känns konstigt eller misstänkt med meddelandet eller erbjudandet? Om ja, vilka varningssignaler kan ni hitta?
- Vad tror ni kan hända om man klickar på länken eller lämnar ut uppgifter?

# Arbetsblad: Tipsrunda

### 1. Svagheter i lösenord

Du hittar ett papper i datasalen där någon har skrivit sitt lösenord: Sofia2009. Vilken är den största svagheten?

A) Det är för kort

B) Det innehåller personliga uppgifter (namn + födelseår)

C) Det är inte unikt

---

### 2. Lösenordsfraser

Vilket av dessa är säkrast men ändå lätt att minnas?

A) P4ssW0rd!

B) katt-Pannkaka-1700-flyger

C) GalDa90?-saX3>d

---

### 3. Tvåfaktorsautentisering (2FA)

En kompis säger: "Jag har 2FA på Instagram, så jag behöver inte tänka på lösenordet." Vad är bästa svaret?

A) Ja, 2FA är så starkt att lösenordet inte längre spelar roll

B) 2FA är ett bra extra skydd, men ett starkt och unikt lösenord är fortfarande grunden

C) Slå av 2FA, det är onödigt krångel

---

### 4. Gratis-appar

Du laddar ner en gratis app för att redigera bilder. Den vill ha tillgång till: kameran, mikrofonen, dina kontakter och platsen du befinner dig på.

Vad är troligast?

A) Appen samlar in mer data än vad den behöver

B) Alla gratis-appar är säkra så länge du bara använder dem för att redigera bilder

C) Gratis-appar använder aldrig din data när den är avstängd

---

### 5. Phishing-mail

Du får ett mail från ”Google Support”: ”Ditt konto stängs om du inte verifierar dig här: http://googl-support-login.com” Vilket är det tydligaste tecknet på att det är bluff?

A) Länken ser konstig ut

B) Google skickar aldrig mail

C) Texten innehåller ordet ”verifiera”

---

### 6. Deepfake-fällan

Du ser en video där en känd influencer säger: ”Swisha 100 kr och få en exklusiv hoodie skickad hem direkt”. Vad är klokast att tänka?

A) Kolla på influencerns officiella konton för att se om erbjudandet finns där

B) Klicka på länken snabbt, innan hoodiesarna tar slut

C) Fråga vänner i chatten om de också har sett videon

---

### 7. Datainsamling

Vilken av dessa är inte ett exempel på att du blir ”produkten” online?

A) Facebook använder dina intressen för att visa riktad reklam

B) Roblox sparar vilka spel du spelar mest

C) Du köper ett datorspel i butik med kontanter

---

### 8. Säkerhetsmedvetenhet

En vän berättar stolt: ”Jag har samma lösenord till alla konton, men det är 18 tecken långt och väldigt svårt att gissa!”. Vad är problemet?

A) Lösenordet är inte svårt att gissa om du vet hans namn

B) Att använda samma lösenord överallt gör att om ett konto hackas, så riskeras alla andra

C) 18 tecken är för långt – svårt att skriva in

---

### 9. Digital stress

Varför skickar bedragare ofta bluffmeddelanden med ord som ”Ditt konto stängs om 2 timmar!”?

A) För att du ska bli stressad och fatta snabba beslut

B) För att det är roligare för dem

C) För att de annars glömmer bort bluffen

---

### 10. Online Community

Din kompis får sitt konto kapat på Discord, och bedragaren skickar länkar till alla i gruppen. Vad är bäst att göra?

A) Klicka för att se om länken verkligen är farlig

B) Ignorera, det är ju inte ditt problem

C) Varna andra i gruppen och tipsa kompisen att kontakta support och byta lösenord

---

## Facit tipsrunda

1. **B) Det innehåller personliga uppgifter (namn + födelseår)**
   Ett av de tydligaste kännetecknen för ett svagt lösenord är att det går att gissa utifrån personlig information. Namn och födelseår är det första en hackare testar, ofta med hjälp av information de hittar på sociala medier. Sofia2009 avslöjar både vem hon är och vilket årtal som är centralt för henne. Alternativ A är delvis relevant – 9 tecken är kortare än rekommenderade 14 – men det största problemet är den personliga informationen. Alternativ C kan man inte avgöra bara genom att se ett lösenord på ett papper.
2. **B) katt-Pannkaka-1700-flyger**
   Det här är en lösenordsfras: lång (24 tecken), blandar bokstäver, siffror och skiljetecken, är svår att gissa – men går att komma ihåg som en absurd bild i huvudet. Alternativ A (P4ssW0rd!) är för kort och bygger dessutom på ett av världens vanligaste lösenord med bara utbytta tecken. Alternativ C (GalDa90?-saX3>d) är också starkt, men i praktiken omöjligt att komma ihåg – och ett lösenord man inte kommer ihåg blir värdelöst.
3. **B) 2FA är ett bra extra skydd, men ett starkt och unikt lösenord är fortfarande grunden**
   2FA är ett extra lås, inte en ersättning för lösenordet. Om lösenordet är svagt eller återanvänt på flera tjänster är det fortfarande en risk – till exempel om en av tjänsterna får en dataläcka, testar hackare samma lösenord på andra platser. Bäst skydd får man genom att kombinera: starkt och unikt lösenord *plus* 2FA. Alternativ A är en vanlig missuppfattning – lösenordet är fortfarande grunden, 2FA är ett tillägg. Alternativ C är fel eftersom 2FA är ett enkelt och effektivt skydd som är väl värt den lilla extra tiden det tar att slå på.
4. **A) Appen samlar in mer data än vad den behöver**
   En bildredigerings-app behöver inte tillgång till dina kontakter eller din plats för att fungera. När en app kräver behörigheter som inte har med dess kärnfunktion att göra är det ofta ett tecken på att företaget vill samla in extra data att sälja vidare eller använda för riktad reklam. Alternativ B är en vanlig missuppfattning – att en app är säker så länge du bara använder den för det den är tänkt till. Men datan samlas in oavsett vad *du* använder appen till. Alternativ C är fel eftersom appar kan samla data även när de inte är i förgrunden.
5. **A) Länken ser konstig ut**
   Den riktiga adressen till Google Support ligger på google.com-domänen. "googl-support-login.com" är en typisk bluffdomän – någon utan koppling till Google har registrerat en adress som ser Google-liknande ut. Det är ett klassiskt phishing-tecken. Alternativ B är fel: Google skickar mail om många saker, bland annat säkerhet. Alternativ C är fel: ordet "verifiera" är inte i sig ett varningstecken – seriösa företag använder det också.
6. **A) Kolla på influencerns officiella konton för att se om erbjudandet finns där**
   En deepfake kan se helt äkta ut, så det räcker inte att lita på hur det ser ut. Det verkliga skyddet är att fråga sig: skulle den här personen verkligen göra det här – och i så fall, borde det inte finnas på hens officiella kanaler? Om erbjudandet inte finns där är det en bluff. Alternativ B är precis vad bedragaren vill: att du agerar snabbt utan att tänka. Alternativ C hjälper inte – dina vänner har sett samma bluff.
7. **C) Du köper ett datorspel i butik med kontanter**
   Att bli "produkten" online betyder att företag samlar in data om dig och tjänar pengar på den – ofta genom att sälja den vidare eller visa riktad reklam. Alternativ A och B är båda exempel på det. Alternativ C däremot lämnar inga

digitala spår: du betalar med pengar och tar hem spelet, och företaget vet inte vem du är. När en tjänst är gratis är du ofta själv produkten – men här betalar du med kontanter.

8. **B) Att använda samma lösenord överallt gör att om ett konto hackas, så riskeras alla andra**
   Även om lösenordet är långt och starkt kan det läcka via en dataläcka på någon av de tjänster han använder – och det händer regelbundet. När det gör det testar hackare samma lösenord på andra tjänster. Har din vän använt samma lösenord på Instagram, Discord, Gmail och Steam räcker det att en drabbas för att alla ska vara i fara. Alternativ A är inte relevant – vi vet inte vad lösenordet är. Alternativ C är fel: 18 tecken är en styrka, inte en nackdel.
9. **A) För att du ska bli stressad och fatta snabba beslut**
   Nätbedrägerier är designade för att spela på våra känslor. Tidsbrist ("2 timmar!"), rädsla ("kontot stängs!") och hetsig ton är alla verktyg för att få dig att agera innan du hinner tänka efter. Det är därför den viktigaste regeln är att stanna upp: så snart något känns brådskande, ta ett steg tillbaka och dubbelkolla. Alternativ B och C är inga verkliga skäl – bedragarna är strategiska och räknar med att stressen leder till klick.
10. **C) Varna andra i gruppen och tipsa kompisen att kontakta support och byta lösenord**
    När ett konto kapas är två saker viktiga: att stoppa spridningen (varna andra så de inte klickar på länkarna) och att hjälpa kompisen få tillbaka kontrollen (kontakta plattformens support, byta lösenord, aktivera 2FA). Alternativ A är farligt – länken kan ladda ner skadlig kod utan att du märker det. Alternativ B lämnar kompisen i sticket och bedragaren fri att skada fler.