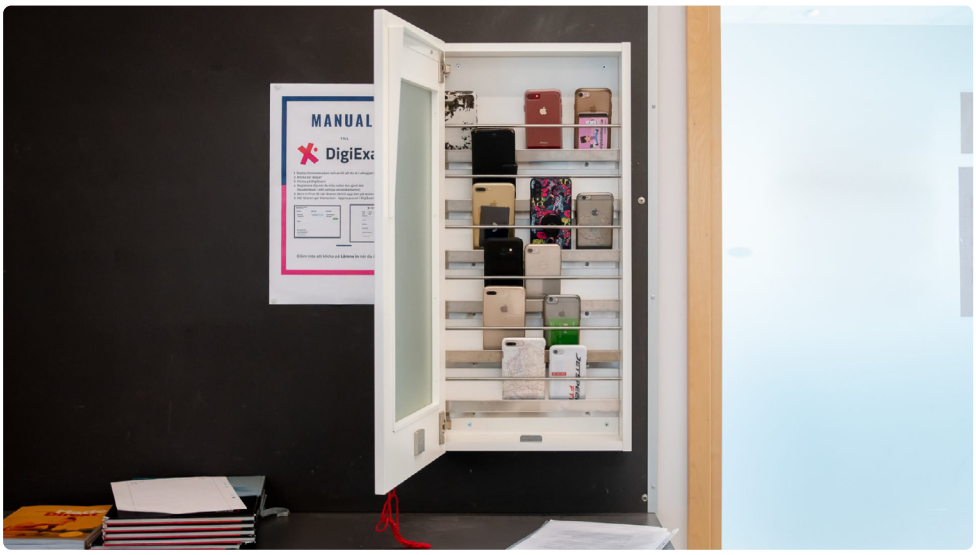
KOLL PÅ REGLER PÅ NÄTET | ÅK 4-6

Tänk säkert - hur säker är din mobil?

Lektionen handlar om att göra elever medvetna om hur de kan bli mer säkra i användningen av sin mobil.

1 Hur viktig är din mobil?



Ta ställning till påståenden, svara ja eller nej.

- Jag använder min mobil varje dag.
- Jag har innehåll på min mobil som ingen annan får komma åt.
- Jag lämnar aldrig ifrån mig min mobil.
- Jag är den enda som kan öppna min mobil.

- Jag uppdaterar regelbundet alla appar på min mobil.
- Jag raderar appar jag inte använder.
- Jag laddar aldrig ner appar som jag inte har hunnit läsa på om.
- Jag har kontroll på vilka av mina appar som har åtkomst till – kan använda – kamera, mikrofon, kontakter och bilder.
- Jag har bilder i min mobil som jag inte vill att någon annan ska se.

- Jag använder samma lösenord på olika tjänster.
- Jag loggar alltid ut från mina sociala medier.
- Jag använder fingeravtryck för att öppna min mobil.
- Jag använder ansiktsigenkänning för att öppna min mobil.
- Jag använder lösenord för att öppna min mobil.

- Jag uppdaterar regelbundet min mobil för att den ska vara säker.
- Jag vet vad jag behöver göra för att spärra eller skydda mina uppgifter om min mobil blir stulen.
- Jag vet vilken mobiloperatör jag har och hur jag kommer i kontakt med dem.

2 Är du säker?

Jämför dina svar från lektionsdel 1 med en kompis.

- Har du och din klasskamrat svarat olika på några påståenden? Vilka?
- Fundera tillsammans kring vad era olika svar kan bero på.
- Vem har mest koll på säkerheten på sin mobiltelefon, du eller din klasskamrat?
- Skriv tillsammans ner vilka fem påståenden som ni tycker det är viktigast att alla som har en mobiltelefon instämmer i.
- Argumentera för varför just de fem påståendena är viktigast.

3 Vad betyder orden?

Använd ett papper och para ihop rätt ord med rätt förklaring.

Ord

a. falska annonser
b. kapa
c. nätfiske
d. phishing
e. ransomeware
f. skadlig kod
g. smishing
h. spionprogram
i. trojan
j. vishing
k. uppdatering
l. virus

Förklaringar

1. Att olovligen och mot din vilja ta kontroll över något, till exempel din dator, din identitet eller ditt betalkort.
2. När någon skickar ett sms för att försöker lura dig att klicka på en länk eller få dig att lämna ifrån dig viktiga uppgifter. Viktiga uppgifter kan till exempel vara ett lösenord eller koden till ett konto.
3. E-postmeddelande där någon ber dig att lämna ifrån dig till exempel inloggningsuppgifter, kontoinformation eller få dig att klicka på en länk. Meddelandet ser ofta ut att komma från ett välkänt företag eller från någon du känner.
4. Ett telefonsamtal från någon som säger att de ringer från till exempel polisen eller ett sjukhus och berättar att något hemskt har hänt. För att lösa det som har hänt vill den som ringer att du ska lämna olika slags uppgifter, exempelvis lösenord, larmkoder eller kontonummer.
5. En form av program som installeras på din dator utan att du märker det när du till exempel klickar på en länk i ett phishing-mail eller tar emot en film eller bild i sociala medier. Programvara kan fungera på olika sätt, men syftet med är alltid att den som har skickat den ska kunna pressa den som drabbas på pengar eller information för att bli av med den.
6. Det du gör när du installerar nya versioner av till exempel apparna i mobilen eller ditt operativsystem i datorn. Viktigt att göra när det finns nya versioner för att vara säker på att säkerheten ska vara så god som möjligt.
7. Ett datorprogram som lurar dig att tro att det är nyttigt, roligt eller bra, men som – när du har installerat och börjat att köra det – visar sig vara skadligt eller göra något helt annat.
8. Kod som tar sig in i dina program och kan skada eller ta kontroll över dem. Ofta handlar skadlig kod om att dina program till exempel börjar samla in data som den som lurat dig får tillgång till, exempelvis lösenord eller inloggningsuppgifter som du använder.
9. Att någon via e-post eller sociala medier försöker få tag i din personliga information, till exempel kortnummer eller lösenord. Det kan till exempel vara någon som ber om dina uppgifter och som ser ut att ha en mejladress från ett företag eller en organisation.
10. Till exempel en tävling där du blir lurad att beställa varor eller skicka in kontouppgifter. Du kanske betalar ett förskott. När du har gjort det försvinner annonsen och du får aldrig det du har beställt.
11. En programvara som samlar in uppgifter från din dator utan att du märker det. Det kan hamna på din dator genom att följa med när du laddar hem eller delar filer. Programmet kan samla information som till exempel dina lösenord och inloggningsuppgifter.