POLITIET
KRIPOS

Til skoleadministrasjonen og lærere

SJEKKLISTE FOR DIGITALE LÆRINGSLØSNINGER

I forbindelse med at et stort antall skoler har tatt i bruk digitale læringsløsninger, har Kripos utarbeidet noen grunnleggende råd som kan bidra til å forhindre at IKT- utstyr og programvareløsninger blir misbrukt. Mange av disse rådene vil også være relevante for elever og deres foresatte og kan med fordel videreformidles til dem.

Om IKT-utstyr

- Sørg for at IKT-utstyret som benyttes til enhver tid er oppdatert med sikkerhets-oppdateringer fra leverandøren, både for operativsystem og programvare. Noen enheter gjør dette automatisk, mens andre må oppdateres manuelt.

- Sørg for at alle antivirusprogram er oppdaterte og aktive.

- Ved bruk av trådløst hjemmenettverk, sørg for at det er kryptert. Hvis det ikke er kryptert, bør du koble deg til internett via mobildata. Det er tre forskjellige nivåer på kryptering av trådløse nett:

    - Åpen (ingen sikkerhet)
    - WEP (lav sikkerhet)
    - WPA/WPA2/WPA3 (høy sikkerhet)

    Det anbefales *ikke* at trådløse nettverk med nivå Åpen eller WEP benyttes, da det har liten eller ingen sikkerhet.

    Avhengig av operativsystem finnes informasjonen på forskjellige steder. Hvis den ikke finnes på stedene nevnt under, anbefales det å ta kontakt med IKT-support eller en datakyndig kollega/venn. Det finnes også mye informasjon om dette på internett, men vær kritisk til veiledningene du finner der. Det skal for eksempel ikke være nødvendig å måtte installere noe for å få sjekket dette på vanlige datamaskiner.

    Enheter med Android operativsystem:
    Innstillinger ➔ WiFi. Velg det trådløse nettverket du er tilkoblet og trykk "Vis". Under fanen "Sikkerhet" vil du finne hvilket nivå det trådløse nettverket har.

    Enheter med MacOS:
    Systeminnstillinger ➔ Nettverk. Velg det trådløse nettverket du er tilkoblet og trykk på "Avansert". Under fanen "Sikkerhet" finner du nivået på det tilkoblede nettverket.

    Enheter med Windows:
    Nederst i høyre hjørne finner du det trådløse nettverket du er koblet til. Trykk på det tilkoblede nettverket, og deretter på "Egenskaper" for å få informasjon om sikkerhetsnivået.

- Ta regelmessige sikkerhetskopier av filer som er viktige for deg. Det kan for eksempel være bilder, dokumenter og regneark som er nødvendig for å utføre viktige arbeidsoppgaver. Sikkerhetskopien bør oppbevares på et sted som ikke er koblet til internett eller de enhetene som er i daglig bruk.

- Hvis det skjer noe unormalt, si i fra til nærmeste leder, virksomhetens sikkerhetspersonell eller IKT-støtte hvis skolen har det. Unormal oppførsel kan for eksempel være at kamera går på uten at du har skrudd det på, at programmer kjører av seg selv eller at maskinen arbeider tungt selv om du bare bruker den til enkle oppgaver.

- Sett på og benytt kameradeksel for å fysisk kontrollere når kameraet på PC'er og andre digitale enheter er på og ikke.

Om videoløsninger

- Foreta noen søk på aktuelle videotjenester for å sjekke om noen har oppdaget sårbarheter eller rapportert om innbrudd på tjenestene.

- Lås møterommet når alle deltakere er på plass for å hindre at uvedkommende kan delta ubemerket.

- Beskytt møterommet med passord. Bytt dette passordet med jevne mellomrom, gjerne fra møte til møte.

- Verifiser at deltakerne er faktiske deltakere og at det ikke er noen blindpassasjerer, f.eks. ved at alle deltagerne presenterer seg med navn og bilde.

- Ha i bakhodet tjenesten kan lagre informasjon som blir delt i chat. Tjenesten kan også lagre filer som deles i løsningen.

- Meld fra til nærmeste leder, virksomhetens sikkerhetspersonell eller IKT-støtte ved unormale hendelser i videoløsningen.

Få mer informasjon på:

https://www.politiet.no/datakriminalitet/
www.nettvett.no
www.datatilsynet.no