**a. Hvordan sikrer bedrifter seg mot phishing, sosial manipulering og andre trusler i kommunikasjon?** Amalie, Vebjørn

Bedrifter kan beskytte seg mot phishing ved å trene ansatte i å gjenkjenne mistenkelige e-poster, bruke flerfaktorautentisering (MFA) for ekstra sikkerhet, og implementere e-postfiltre som blokkerer skadelige meldinger. Det er også viktig å ha klare sikkerhetspolicyer som forbyr klikk på ukjente lenker og deling av sensitiv informasjon via e-post. Regelmessige oppdateringer av programvare bidrar til å tette sikkerhetshull, og simuleringer av phishing-angrep kan styrke beredskapen og bevisstheten blant ansatte.

Bedrifter må beskytte seg mot sosial manipulering av å være obs på hvem som sender for eksempel en email, fordi hvis det er link basert kan det være virus eller andre skadelige programvarer.

Man må også være forsiktig med nettsider.

Sjekk om nettsiden eller emailen kan stoles på.

Selv med opplæring slipper noen phishing-angrep og sosial manipulering gjennom, fordi de ofte ser troverdige ut. Det er heller ikke like lett for alle å forstå tekniske sikkerhetsprotokoller, noe som kan gjøre opplæring utfordrende. I tillegg kan strenge sikkerhetstiltak føles tungvinte, og da er det fort gjort at folk begynner å ignorere dem. Bedrifter må derfor finne en balanse mellom sikkerhet, brukervennlighet og tilpasset opplæring.

**b. Lag en kort oppsummering med eksempler på gode rutiner.** emirhan, Ådne

Det er kjempeviktig å ha gode rutiner. For å beskytte seg mot phishing og sosial manipulering må bedrifter trene ansatte til å gjenkjenne svindelforsøk, bruke sikkerhetstiltak som e postfiltering og tofaktorautentisering, og ha klare regler for hvordan man håndterer mistenkelige forespørsler.

Ansatte bør alltid dobbeltsjekke viktig informasjon og rapportere mistenkelig aktivitet for å forhindre svindel.