IT-håndbog for NEG elever

Indhold

IT-sikkerhed på NEG 3
Din computer og dine enheder 4
Login og adgangskoder 5
Vælg en stærk adgangskode 5
Hold dit login personligt 5
Sikker brug af internettet 6
Kontrollér hjemmesider 6
Download og installation af programmer 6
Genkend digital svindel 7
Sådan genkender du mistænkelige beskeder 7
Sådan håndterer du mistænkelige beskeder 7
Beskyt dine og andres personlige oplysninger 8
Skolens netværk og udstyr 9
Brug af skolens Wi-Fi 9
Brug af skolens computere og udstyr 9
Hvad gør du ved et sikkerhedsproblem? 10
Huskelisten ..... **Fejl! Bogmærke er ikke defineret.**

IT-sikkerhed på NEG

Alle elever har et ansvar for at bidrage til et sikkert IT-miljø på NEG. Din adfærd er med til at beskytte både dig selv, dine medelever og skolen. Når du bruger skolens IT-systemer, skal du følge skolens regler og anvisninger.

De vigtigste grundregler er:

- Brug kun dit eget skolelogin, og hold dine adgangskoder hemmelige.
- Vær kritisk over for hjemmesider, mails, SMS'er og links.
- Download ikke ukendte filer, og installer ikke programmer uden tilladelse.
- Beskyt dine egne og andres personlige oplysninger.
- Hold dine enheder opdaterede, og lås dem, når du ikke bruger dem.
- Pas på skolens IT-udstyr, og følg skolens regler omkring brugen af dem.
- Kontakt IT-support eller din underviser, hvis du opdager et sikkerhedsproblem.

IT-sikkerhed er et fælles ansvar. Din adfærd er med til at beskytte både dig selv og dine medelever på NEG.

Din computer og dine enheder

Din computer og mobiltelefon indeholder ofte personlige oplysninger og giver adgang til dine konti og skolens systemer. Derfor er det vigtigt, at dine enheder er beskyttede og opdaterede.

Brug et styresystem, der fortsat modtager sikkerhedsopdateringer, og sørg for at installere opdateringer til både styresystem og programmer. Enhedens indbyggede sikkerhedsfunktioner skal være aktiverede, og du bør altid bruge en skærmlås med adgangskode, PIN-kode eller biometrisk låsning.

Installer kun programmer og apps fra kilder, du har tillid til. Vær opmærksom på, hvilke tilladelser apps beder om, og undersøg nærmere, hvis et program eller en hjemmeside kræver, at du deaktiverer sikkerhedsfunktioner.

Lås din enhed, når du ikke bruger den, og undgå at efterlade den uden opsyn. Hvis du mister en telefon eller computer, der bruges til skolens login eller indeholder oplysninger fra skolen, skal du hurtigst muligt kontakte skolens IT-support.

Er du i tvivl om, hvorvidt din computer kan bruges til skolens programmer, kan du spørge din underviser eller IT-support.

Login og adgangskoder

Dit skolelogin giver adgang til skolens systemer og oplysninger. Derfor skal du beskytte både dit brugernavn og din adgangskode.

Vælg en stærk adgangskode

En god adgangskode er lang, unik og svær for andre at gætte. Brug mindst 12 tegn, og vælg en adgangskode, du ikke bruger andre steder. Undgå navne, fødselsdatoer og andre personlige oplysninger. En lang adgangskode bestående af flere tilfældige ord kan være et godt valg, og du behøver ikke nødvendigvis erstatte bogstaver med tal eller specialtegn for at gøre den sikker.

Du kan med fordel bruge en sikker adgangskodeadministrator til at opbevare dine adgangskoder.

Hold dit login personligt

Du må aldrig dele din adgangskode med andre, lade andre bruge din konto eller logge ind for en anden elev. Du må heller ikke bruge andre elevers login. Selv hvis en ven beder om at låne dit login, skal du sige nej.

Når flere personer bruger samme konto, kan det være svært at afgøre, hvem der har udført en bestemt handling. Det kan skabe problemer ved fejl eller misbrug.

IT-kriminelle forsøger at genbruge adgangskoder, der er stjålet fra andre tjenester. Hvis du bruger den samme adgangskode flere steder, kan et sikkerhedsbrud ét sted derfor give adgang til dine andre konti.

Hvis du har mistanke om, at andre kender din adgangskode, skal du ændre den hurtigst muligt og kontakte skolens IT-support.

Sikker brug af internettet

Når du bruger internettet på NEG, skal du følge skolens regler og være opmærksom på, hvilke hjemmesider du besøger, og hvilke filer du henter.

Kontrollér hjemmesider

Inden du indtaster adgangskoder eller andre oplysninger, skal du kontrollere, at du er på den rigtige hjemmeside. Se på webadressen, og vær opmærksom på stavefejl, usædvanlige adresser og sider, der forsøger at presse dig til at handle hurtigt.

Et hængelåsikon eller HTTPS i adressen betyder, at forbindelsen er krypteret. Det er dog ikke en garanti for, at hjemmesiden er troværdig. Falske hjemmesider kan også bruge krypterede forbindelser.

Vær desuden forsigtig med pop op-vinduer, konkurrencer og tilbud, der virker for gode til at være sande.

Download og installation af programmer

Filer og programmer fra internettet kan indeholde virus eller andre skadelige funktioner. Download derfor kun filer fra kilder, du har tillid til, og åbn ikke filer, du ikke forventer at modtage.

Du må ikke installere spil eller anden software på skolens udstyr uden tilladelse. Hvis du skal bruge et bestemt program i undervisningen, men er usikker på, om det er sikkert, skal du spørge din underviser eller skolens IT-support. Du må ikke slå sikkerhedsfunktioner fra for at få et program til at virke.

Download, opbevaring og deling af ulovligt materiale eller materiale i strid med ophavsretten er ikke tilladt. Skolens netværk og systemer må heller ikke bruges til ulovlige aktiviteter.

Genkend digital svindel

Digital svindel foregår blandt andet via e-mails, SMS'er, sociale medier og beskeder i apps. Svindlere forsøger ofte at få dig til at udlevere oplysninger, åbne skadelige filer eller besøge falske hjemmesider.

En besked kan udgive sig for at komme fra NEG, en underviser, en bank, et fragtfirma, en offentlig myndighed eller en person, du kender.

Sådan genkender du mistænkelige beskeder

Vær særligt opmærksom, hvis en besked:

- Beder om adgangskoder, betalingsoplysninger eller andre fortrolige oplysninger.
- Truer med at lukke din konto eller påstår, at en pakke ikke kan leveres, medmindre du reagerer hurtigt.
- Indeholder uventede links, vedhæftede filer eller anmodninger om betaling.
- Kommer fra en afsenderadresse eller et telefonnummer, der virker forkert, eller indeholder usædvanlige formuleringer.

En besked kan godt være falsk, selvom sproget er korrekt, og afsenderens navn ser rigtigt ud.

Sådan håndterer du mistænkelige beskeder

Klik ikke på links, og åbn ikke vedhæftede filer, hvis du er usikker på beskedens indhold. Kontrollér afsenderens fulde e-mailadresse, hvis det er en mail, og kontakt afsenderen via en anden, kendt kontaktvej, hvis du er i tvivl.

Hvis beskeden tilsyneladende kommer fra en underviser eller medstuderende, men indeholder en usædvanlig anmodning, skal du sikre dig, at den faktisk kommer fra vedkommende. Du kan i stedet gå direkte ind på organisationens officielle hjemmeside frem for at bruge et link i beskeden.

Du må aldrig oplyse din skoleadgangskode eller andre fortrolige loginoplysninger via e-mail eller beskeder. Slet eller rapportér mistænkelige beskeder efter skolens anvisninger.

Hvis du allerede har klikket på et mistænkeligt link eller indtastet dine oplysninger, skal du straks kontakte skolens IT-support.

Beskyt dine og andres personlige oplysninger

Personlige oplysninger kan eksempelvis være dit CPR-nummer, din adresse, dit telefonnummer, dine loginoplysninger, billeder eller oplysninger om andre personer. Du skal være opmærksom på, hvilke oplysninger du deler, og hvem der får adgang til dem.

Del kun oplysninger, når der er et reelt behov. Send ikke følsomme oplysninger gennem almindelig e-mail, medmindre der anvendes en godkendt og sikker løsning. Hvis du skal sende fortrolige oplysninger i forbindelse med undervisningen eller administrationen, skal du bruge den løsning, NEG har anvist. Kontakt skolens administration, hvis du er i tvivl om, hvordan oplysningerne skal sendes sikkert.

Du må ikke dele andres personlige oplysninger, billeder eller dokumenter uden tilladelse. Vær også opmærksom på, hvad du offentliggør på sociale medier og andre hjemmesider. Oplysninger og billeder kan blive kopieret eller delt videre, selvom du senere sletter dem.

Kontrollér desuden, hvem der har adgang til de dokumenter og filer, du deler. På den måde mindsker du risikoen for, at oplysninger ender hos uvedkommende.

Skolens netværk og udstyr

NEG stiller trådløst netværk, computere og andet IT-udstyr til rådighed for elever og ansatte. Du skal følge skolens anvisninger og behandle udstyret ansvarligt.

Brug af skolens Wi-Fi

Når du bruger skolens trådløse netværk, skal du vælge det netværk, NEG har anvist til elever, og følge skolens anvisninger om netværk og login. Undgå at indtaste følsomme oplysninger på netværk, du ikke har tillid til, og kontakt IT-support, hvis du er i tvivl om, hvilket netværk du skal bruge.

Et åbent netværk er ikke nødvendigvis sikkert til alle formål. Du skal derfor altid være opmærksom på, hvilke oplysninger du sender over netværket.

Brug af skolens computere og udstyr

Skolens udstyr er beregnet til undervisning og andre skoleaktiviteter. Du må ikke installere programmer eller spil uden tilladelse, ændre sikkerhedsindstillinger, forsøge at omgå skolens begrænsninger eller få adgang til andre elevers filer og konti. Du må heller ikke bruge udstyret til ulovlige aktiviteter eller fjerne det fra skolen uden tilladelse.

Du skal passe på udstyret og melde fejl eller skader til din underviser eller skolens administration. Hvis udstyr beskadiges, forsvinder eller bliver stjålet, skal det meldes hurtigst muligt.

Når du bruger en computer, som andre også har adgang til, skal du låse den, hvis du forlader den, og logge ud af skolens systemer, når du er færdig. Det forhindrer andre i at få adgang til din konto og dine oplysninger.

Misbrug eller beskadigelse af skolens udstyr kan få konsekvenser efter skolens gældende regler.

Hvad gør du ved et sikkerhedsproblem?

Det er vigtigt, at du reagerer hurtigt, hvis du opdager noget mistænkeligt. Det gælder eksempelvis, hvis du har indtastet dine oplysninger på en mistænkelig hjemmeside, åbnet en skadelig fil, modtager loginanmodninger, du ikke selv har startet, eller opdager, at andre bruger din konto.

Du skal også reagere, hvis din computer pludselig opfører sig anderledes end normalt, eller hvis du mister en enhed, der indeholder oplysninger fra skolen.

Stop med at bruge det mistænkelige link, program eller den pågældende tjeneste.
Undlad at forsøge at løse problemet ved at installere programmer eller ændre sikkerhedsindstillinger på egen hånd. Kontakt straks skolens IT-support eller din underviser, og forklar, hvad der er sket.

Hvis du har oplyst din adgangskode, skal du fortælle det til IT-supporten, så de kan hjælpe med at sikre din konto. Følg derefter skolens anvisninger om, hvad du skal gøre.

Du skal ikke være bange for at melde en fejl eller et klik på et forkert link. Det vigtigste er, at NEG får besked så hurtigt som muligt, så problemet kan begrænses.