Guide til IT-sikkerhed for andelshavere

Indholdsfortegnelse

(sidst opdateret 26/4 2023)

Introduktion

Dette er en guide der skal hjælpe dig som andelshaver til at følge gode IT-sikkerhedsprincipper, som vi også anvender i Vindenergi Danmark. Jo flere af principperne og rådene du kan følge i din digitale færden, jo bedre. Selvom nogle råd og principper ikke nødvendigvis er vigtigere eller bedre end andre, så har vi forsøgt at prioritere i dem for dig. Dette betyder, at de emner der står først, enten er de vigtigste eller nemmeste for dig at efterleve, mens dem længere nede på listen er mere avancerede, men ikke desto mindre, stadig yderst relevante.

Den korte opsummerede udgave kan koges ned til følgende punkter:

- Anvend adgangskoder med minimum 16 karakterer, med mindst ét stort og lille bogstav, mindst ét tal, og mindst ét specialtegn. Genanvend aldrig et password, og brug en password manager. Vindenergi Danmark anbefaler 1Password.
- Del aldrig din adgang til Vindenergi Danmarks selvbetjeningsportal med nogen, og log aldrig på den fra enheder og netværk som ikke er dine egne.
- Anvend MFA eller 2FA alle steder hvor det er muligt.
- Kontrollér at websider og domæner er korrekte, undgå phishing og svindel via e-mail, SMS og telefonopkald ved at være kritisk, og via uafhængig verificering. Vær forsigtig med offentlige computere og Wi-Fi, lås enheder, og vær generelt kritisk over for informationer på nettet.
- Hold dit operativsystem, software, og apps til en hver tid opdateret. Kontrollér at alt software, og browser plugins er fra pålidelige kilder. Anvend en ad blocker til din browser. Vindenergi Danmark anbefaler uBlock Origin.
- Sørg for at du har et aktivt antivirus program som løbende bliver opdateret, og at du har en aktiv firewall.
- Ændre potentiel standard bruger og adgangskode i dit netværksudstyr.

Adgangskoder / passwords

Adgangskoder er nøglen til at beskytte dine personlige oplysninger og onlinekonti. En stærk adgangskode bør være mindst 16 tegn lang og indeholde en blanding af små og store bogstaver, tal og specialtegn. Eksempler på specialtegn kan være, men ikke begrænset til, udråbstegn (!), spørgsmålstegn (?), procenttegn (%), og &-tegn. Se infografikken nedenfor, over hvor lang tid det tager at bryde adgangskoder af varierende længde, og hvorfor et minimum på 16 er nødvendigt for at have et nogenlunde fremtidssikret password i et par år frem.
For at sikre bedst mulig beskyttelse, bør du aldrig bruge den samme adgangskode mere end ét sted.

Årsagen til dette, kan følgende tænkte (men ikke usandsynlige) eksempel illustrere. Antag at den e-mail og adgangskode du anvender til Facebook, er den samme som den du anvender til Vindenergi Danmarks selvbetjeningsportal. Der sker så det, at Facebook bliver hacket, og hackerne lægger alle e-mail og password kombinationer fra Facebook ud på det mørke internet (dark web). Dette betyder ikke kun at andre ondsindede personer nu kan tage din e-mail og dit password, og prøve dem alle de steder de lyster, herunder også Vindenergi Danmarks selvbetjenings portal. Det betyder også at dit password nu kommer til at indgå i de password lister, som programmer der er designet til at bryde ind i systemer anvender. Det betyder så igen, at hackere som ikke specifikt går efter dig, men bare bruger programmerne til at bryde ind steder, nu også afprøver din e-mail og dit password automatisk alle de steder de forsøger at bryde ind. Lige pludselig har en teenager et sted i verden, som har leget med en af disse programmer, adgang til at ændre hvilken konto din(e) udbetaling(er) fra din(e) vindmølle(r) skal indbetales på af os, via Vindenergi Danmarks selvbetjening. Det er

udelukkende dit ansvar at sikre, at det kun er dig der har adgang til selvbetjeningen.
Disse dage sker det i øvrigt desværre ret ofte, at større virksomheder som vi betragter som sikre, bliver hacket.

Et nyttigt værktøj til at kontrollere, om din e-mail (og tilhørende adgangskode) er blevet lækket i et kendt hack, er haveibeenpwned.com. Her kan du indtaste din e-mailadresse, og se om den er blevet kompromitteret. Hvis det er tilfældet, er det vigtigt at ændre den adgangskode, og alle der minder om den, hurtigst muligt.

At skulle have forskellige adgangskoder alle de mange steder man skal bruge sådan en, kan gøre det svært at huske dem. Derfor kan en password manager, såsom 1Password, hjælpe dig med at opbevare og holde styr på alle dine adgangskoder. Den kan også generere stærke adgangskoder, så du ikke skal bekymre dig om hvorvidt koderne er gode. En anden fordel er, at du kun skal huske én adgangskode, nemlig koden til din password manager. Denne ene adgangskode, eller adgangssætning, skal til gengæld være god.

Adgangssætninger er en anden metode til at lave sikre adgangskoder, som er nemmere at huske. En adgangssætning er en kombination af flere ord, der danner en sætning. For eksempel: "Mine2$HundeElskerAtLøbe1TurISkoven!". Sætninger kan være nemmere at huske og sværere for hackere at gætte eller bryde. Nedenfor giver jeg et eksempel på, hvordan man kan lave en adgangssætning som er nem at huske, men svær at bryde med konventionel computerkraft i mange år frem.

Find en sætning som er nem for dig at huske. Det skal ikke være en ikke velkendt sætning, som er brugt mange steder. Dvs. ingen populære film citater, produkt slogans, eller lignende.
For nogle år siden, havde en café i Aarhus et navn på en drink som var svær at glemme. Drinken eksisterer ikke længere, men den hed:

”Dengang Katrine blev voksen og stadig ønskede sig en hest.”

Tager vi udgangspunkt i denne sætning, kunne man lave den om til en adgangssætning der er lige så nem at huske.
Først kan man fjerne alle mellemrummene, og skrive hvert start bogstav med stort. Derefter kan man udskifte navnet med et andet, som ikke er et navn på en person der har tæt tilknytning til en selv. Dette vil sige, at man ikke skal anvende et navn fra ens tætte familie, eller navne på ens kollegaer. Man kan så udskifte de ord der nemt kan udskiftes med tal i stedet for, som f.eks. ”en hest” til ”1Hest”. Igen herefter, kan man kigge på, om der er andre nemme ændringer, som kan gøre det sværere at gætte, men ikke sværere at huske. Dette kan være at ændre ”ø” til ”oe”. For at få lidt flere tal i spil, kan man lave en regel om at udskifte f.eks. alle ”a” med ”4” i stedet for, da ”4” ligner lidt et ”A”. Sidst men ikke mindst, kan man inkludere et par specialtegn. Der kan man f.eks. erstatte ”og” med &, som jo giver samme mening, og så kan man lave hele sætningen om til et spørgsmål. Så kunne man få følgende:

”Deng4ngCh4rlotteBlevVoksen&St4digOenskedeSig1Hest?”

Dette er en yderst stærk adgangssætning. Den behøves selvfølgelig ikke at være så lang og kompleks, men fordelen ved sætninger er at man nemmere kan gøre dem længere end enkelte ord. Jo flere normale ordbogsord man bruger i ens sætning, jo vigtigere er det er få lidt længde på den. Dette eksempel var blot for at give inspiration, og ikke den eneste måde hvorpå man kan lave gode adgangssætninger eller adgangskoder.

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

HIVE SYSTEMS

› Learn how we made this table at hivesystems.io/password

Vindenergi Danmarks selvbetjeningsportal

Dit login til Vindenergi Danmarks selvbetjeningsportal er personligt, og må ikke deles med andre. Din adgangskode skal være stærk (genlæs evt. afsnittet om adgangskoder), og du bør kun logge på den fra dine egne enheder, og kun fra egne netværk.
Har du af den ene eller anden årsag brug for, at flere personer kan logge på din konto, så kan du oprette en specifik brugerkonto til dette. Denne konto kan så tildeles de rettigheder som lige netop er nødvendig for at personen kan udføre den specifikke tiltænkte rolle. Ser vi at en konto bliver benyttet af flere personer, så kan vi af sikkerhedsmæssige årsager finde på at låse kontoen. Det er dit ansvar som andelshaver, at uvedkommende ikke får adgang til din konto.
Er du i tvivl om noget omkring vores selvbetjening, så er det bedre du kontakter os, end at du antager noget er i den skønneste orden hvis det ikke er. Vi vil også hellere have at du rapporterer noget underligt/mistænkeligt en gang for meget, end en gang for lidt, også selvom det viser sig der ikke var en årsag til bekymring.

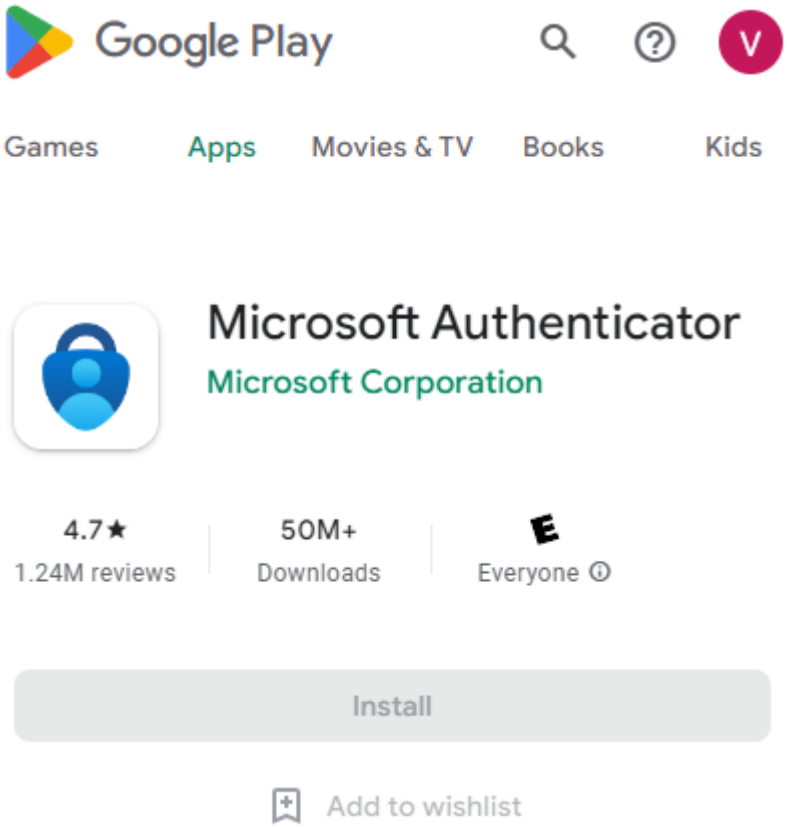
To-faktor (2FA) / multi-faktor (MFA) autentificering

To-faktor autentificering (2FA) eller flerfaktor autentificering (MFA) er en ekstra sikkerhedsforanstaltning, der kræver mere end blot en adgangskode for at få adgang til dine onlinekonti. Ved at aktivere 2FA/MFA øger du sikkerheden betydeligt, fordi det gør det meget sværere for uautoriserede personer at få adgang til dine konti, selv hvis de har din adgangskode.

Det er en god idé at aktivere 2FA/MFA, hvor det er muligt. Specielt vigtigt på e-mail, bankkonti, sociale medier og andre tjenester, der indeholder følsomme oplysninger. Mange tjenester tilbyder denne mulighed og det er nemt at sætte op.

Vi anbefaler at bruge en authenticator-app som Microsoft Authenticator, når du bruger 2FA/MFA. Denne app genererer engangskoder, der skal indtastes sammen med din adgangskode, når du logger ind på en konto. Fordi koderne skifter med jævne mellemrum og kun er gyldige i en kort periode, vil det være meget sværere for en hacker at få adgang til dine konti, selv hvis de kender din adgangskode.

Authenticator-apps som Microsoft Authenticator er generelt mere sikre end andre 2FA-metoder, såsom SMS-koder, fordi de ikke kan blive opsnappet eller omgået så nemt. Når du har installeret appen på din smartphone eller tablet, kan du nemt koble den til dine onlinekonti ved at følge tjenestens vejledning for at aktivere 2FA/MFA.



(sidst opdateret 26/4 2023)

Awareness og sikker internet adfærd

Dette afsnit handler om gode principper når man bevæger sig på internettet. Disse er afgørende for at beskytte dine personlige oplysninger, og undgå at blive et offer for cyberkriminalitet. Nedenfor gennemgås nogle af de emner, som du skal være særligt opmærksomme på.

Websider og deres domæne

Kontrollér altid at den side du er på, har det domænenavn du forventer (eksempel: mitid.dk og IKKE mit-id.dk), og at der er et hængelås-ikon i adresselinjen på din browser. Dette indikerer, at hjemmesiden bruger en sikker forbindelse (HTTPS), og at dine data bliver krypteret, når de sendes mellem din browser og hjemmesiden. Dette er specielt vigtigt på sider hvor du logger ind, betaler med dine kortoplysninger, eller på anden vis overfører sensitive informationer.
Vær opmærksom på eventuelle stavefejl eller andre uregelmæssigheder i domænenavnet, da det kan være tegn på en falsk hjemmeside.
Har du behov for at downloade filer, så sørg for at du kun gør det fra velkendte websider, og at du virusscanner dem efter download.

Phishing og svindel

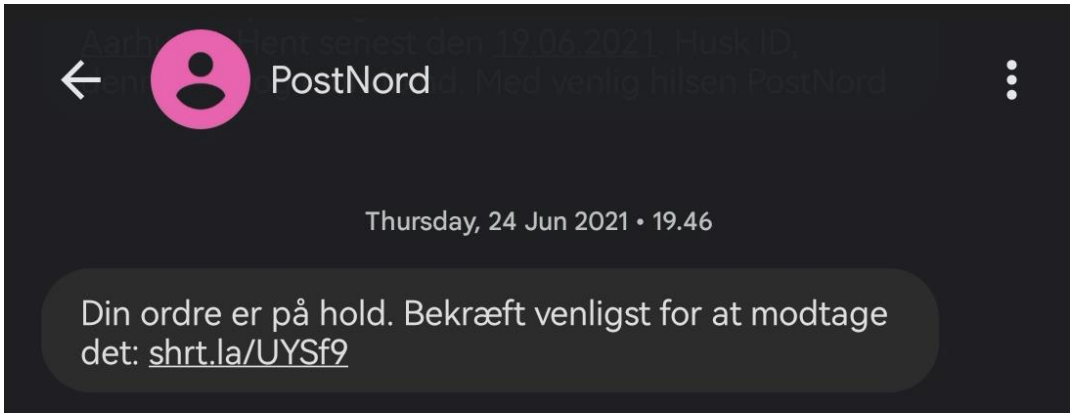
Vær opmærksom på phishing-forsøg (e-mail), smishing-forsøg (SMS), telefonopkald, eller andre former for svindel, der forsøger at narre dig til at give dine personlige oplysninger, adgangskoder, kreditkort oplysninger, eller betalinger generelt. Størstedelen af cyberkriminalitet, foregår ved at man forsøger at narre menneskerne, da de ofte er nemmere at narre end maskinerne.

E-mail

Kontroller altid at afsenderadressen i de e-mails du modtager stemmer overens ift. hvem afsenderen udgiver sig for at være. Læg mærke til smådetaljer, da de kan betyde om noget er reelt eller svindel. For eksempel er det nemt at overse at micrrosoft.com ikke er det samme som microsoft.com.
Derudover er det værd at notere sig, at det er sjældent reelle virksomheder og instanser beder dig følge et link i e-mailen, for derefter at logge ind og verificere din konto. Kommer du ud for at du i en mail bliver bedt om at besøge et link, så er det markant bedre, at du manuelt åbner browseren, og indtaster adressen selv. På den måde er du helt sikker på, at du kommer ind på den korrekte webside.
E-mail kan også indeholde vedhæftninger i form af filer. Her skal man være specielt varsom, især hvis det drejer sig om applikations filer (blandt andet .exe filer). Alle filer man modtager på mails, bør man sørge for at scanne med sit antivirus software. Vil man være helt sikker, kan man også scanne dem via virustotal.com, som sørger for at scanne filen med flere forskellige sikkerhedsprodukter på én gang.

SMS / tekstbeskeder

Forsøg på at svindle dig, kan også komme via SMS beskeder. Det er muligt for en afsender, selv at både angive telefonnummer ved opkald, og afsender navn ved SMS-beskeder. Dette betyder, at vælger en afsender f.eks. Postnord som navn, vil den SMS havne i din SMS-tråd sammen med andre reelle beskeder fra Postnord. Kommer du til at trykke på et link i en SMS, hvor du bliver bedt om at downloade en app uden om det officielle Play Store (Android) eller App store (Apple), så lad være med det. Alle reelle og officielle virksomheder udgiver deres apps via de officielle stores.
Skulle du nogensinde modtage en SMS fra Vindenergi Danmark, hvor du er i tvivl om det er os der har sendt den, så kontakt os hellere end gerne og få det be- eller afkræftet.



(eksempel på hvordan en smishing SMS kan se ud)

Telefonopkald

Stol ikke på folk der ringer til dig, og udgiver sig for at være noget du ikke er sikker på de er. Siger de f.eks. at de er fra Microsoft, politiet, SKAT, eller lignende, så spørg dem efter deres navn og arbejdstelefonnummer. Ring så til den pågældende instans' hovednummer op, og bed om at snakke med den pågældende person. Udlever aldrig sensitive informationer af nogen art, til personer du ikke har verificeret, er hvem de udgiver sig for at være. Dette gælder også Vindenergi Danmark. Er du i tvivl om det er en Vindenergi Danmark medarbejder som kontakter dig, så ring til vores hovednummer på 7632 1919 og spørg efter den pågældende person.

Offentlige computere

Det er bedst at undgå at logge ind på dine personlige konti fra offentlige computere, såsom dem på biblioteker og internetcaféer. Disse computere kan være inficeret med malware eller have overvågningssoftware installeret, der registrerer dine adgangskoder og andre følsomme oplysninger. Hvis du er nødt til at bruge en offentlig computer, sørg for at logge ud af alle dine konti og slette browserhistorikken og cookies, før du forlader computeren. Når du kommer hjem igen, så opdatér de(n) pågældende adgangskode(r).
Drejer det sig om en bibliotekscomputer, hvor man har brug for at printe, så er det bedre at have det man skal printe med på et USB-stik.

Offentlige Wi-Fi netværk

Undgå at bruge offentlige, gratis Wi-Fi-netværk, især til følsomme aktiviteter som netbank, indkøb, og brug af Vindenergi Danmarks selvbetjening. Disse netværk er ofte usikre og kan let udnyttes af hackere til at opsnappe dine data. Hvis du er nødt til at bruge et offentligt Wi-Fi-netværk, skal du sørge for at være forsigtig og undgå at indtaste personlige oplysninger samt adgangskoder, eller også anvende en end-to-end krypteret VPN-forbindelse.
Som alternativ til et offentligt Wi-Fi, kan man anvende sin smartphones hotspot funktionalitet. Dette er altid bedre end at logge på et usikkert Wi-Fi.

Låsning af computer og smartphone

Det er en god idé at låse sin computer og smartphone, når man går fra den. Dette beskytter dine data og forhindrer uautoriseret adgang til dine personlige oplysninger og konti. På de fleste computere kan du låse computeren ved at trykke på en tastekombination (f.eks. Windows-tast + L på en Windows-computer eller Control + Command + Q på en Mac). Når din computer er låst, skal du indtaste din adgangskode eller bruge en anden godkendelsesmetode for at få adgang til den igen. Ved smartphones kan du beskytte dem med en adgangskode, pinkode eller biometrisk sikkerhed, såsom fingeraftryk eller ansigtsgenkendelse.

Generelt set skal man være kritisk overfor alt man oplever på nettet. Alle med adgang til internettet kan publicere informationer. Som med alt andet, hvis noget lyder for godt til at være sandt, så er der risiko for at det ikke er sandt. Er du i tvivl om noget, så dobbelttjek det via en anden kilde.

Operativ- og styresystem (Windows, macOS, Linux, osv.) samt generel software

En af de vigtigste aspekter ved IT-sikkerhed er at holde sit operativsystem og sin software opdateret. Producenter frigiver regelmæssigt opdateringer og rettelser, der omfatter sikkerhedsforbedringer, fejlrettelser og nye funktioner. Disse opdateringer beskytter mod kendte sårbarheder og hjælper med at sikre, at dine systemer og programmer fungerer korrekt og effektivt.

Opdateringer til dit operativsystem og software kan ofte installeres automatisk, men det er en god idé at tjekke manuelt for opdateringer regelmæssigt. For Windows kan du finde opdateringsindstillingerne i "Indstillinger" under "Opdatering og sikkerhed". På en Mac kan du finde opdateringer i "Systemindstillinger" under "Softwareopdatering". Linux-brugere kan opdatere deres systemer via kommandolinjen eller ved hjælp af en pakkehåndteringsapplikation, afhængigt af distributionen.

Ud over at holde operativsystemet opdateret, er det også vigtigt at opdatere sine installerede programmer og applikationer (dette gælder også for apps på sin smartphone). Mange programmer har en indbygget funktion til at søge efter opdateringer, som kan findes i programindstillingerne eller menuen "Hjælp". Hvis en sådan funktion ikke er tilgængelig, kan man besøge programmets officielle hjemmeside for at finde opdateringer og installationsinstruktioner.
Det er også vigtigt at være opmærksom på, hvilken software man installerer på sin computer. Download kun programmer og applikationer fra velrenommerede kilder, og vær opmærksom på eventuelle tilladelser eller adgangsrettigheder, som softwaren anmoder om. Vær særligt forsigtig, når du installerer gratis software, da det kan medføre uønsket software eller skadelige programmer.

Ved at følge disse retningslinjer og holde dit operativsystem og software opdateret, kan du reducere risikoen for IT-sikkerhedsproblemer og beskytte dine data og personlige oplysninger.

Backup af dine data er også en vigtig del af generel IT-sikkerhed. Sikkerhedskopiering sikrer, at du har en kopi af dine vigtige filer og oplysninger, hvis der skulle opstå et problem, såsom datatab, hardwarefejl eller ransomware-angreb. Du bør oprette en plan for regelmæssig sikkerhedskopiering og bruge pålidelige metoder, såsom eksterne harddiske, cloud-tjenester eller specialiserede backup-programmer.

Desuden er det vigtigt at være opmærksom på de tilladelser og adgangsrettigheder, som du giver til de programmer og applikationer, du installerer. Nogle applikationer kan anmode om adgang til dine personlige oplysninger, kamera, mikrofon eller placering, selvom det ikke er nødvendigt for deres funktion. Vær kritisk over for disse anmodninger og giv kun tilladelse, hvis det er absolut nødvendigt for applikationens formål. Dette råd gælder både for computere, tablets, og smartphones.
Endelig er det vigtigt at være opmærksom på de potentielle trusler, der kan opstå, når du bruger forskellige former for software og tjenester. For eksempel kan nogle browserudvidelser indeholde skadelig kode eller opsnappe dine data uden din viden. Vær forsigtig, når du installerer browserudvidelser, og læs anmeldelser og omtaler for at sikre, at udvidelsen er sikker og pålidelig.

En af de browserudvidelser som vi anbefaler hos Vindenergi Danmark, udover den tidligere nævnte password manager 1Password, som også eksisterer som browser plugin, er en ”ad blocker”. Dette

kunne være uBlock Origin som er en browserudvidelse, der hjælper med at blokere reklamer og beskytte brugernes privatliv ved at blokere indhold, der sporer deres aktiviteter på internettet. Når uBlock Origin er installeret og aktiveret i en browser, vil den analysere hver webside, der besøges, og blokere annoncer, trackers og andre former for indhold, der kan forringe brugeroplevelsen eller udgøre en sikkerhedsrisiko.
uBlock Origin har en liste over kendte reklamenetværk og blokerer deres annoncer. Det har også muligheden for at blokere scripts og cookies, som kan spore brugerens adfærd på internettet. Samlet set hjælper uBlock Origin med at forbedre hastigheden på websider og beskytte brugerens privatliv ved at blokere uønsket indhold og sporingsteknologier.

Antivirus og firewall

Antivirus

Antivirus- og antimalware-software er en anden vigtig del af din generelle IT-sikkerhed. Disse programmer beskytter din computer mod skadelige programmer og trusler og kan bidrage til at opdage og fjerne malware, før det kan forårsage skade. Sørg for enten af have den indbyggede antivirus i operativsystemet aktiveret, som f.eks. Microsoft Defender når det drejer sig om Windows, eller installér en pålidelig antivirus- eller antimalware-løsning og hold den opdateret med de seneste signaturfiler og definitioner.

Firewall

De fleste moderne operativsystemer, som Windows og macOS, har en indbygget firewall, der normalt er aktiveret som standard. Det er vigtigt at sikre, at din firewall er aktiveret og korrekt konfigureret for at beskytte din computer effektivt.

Hjemmenetværk – router/modem og Wi-Fi

Hjemmenetværk og routere spiller en vigtig rolle i vores daglige internetbrug, da de giver os adgang til internettet og muliggør kommunikation mellem forskellige enheder i hjemmet. For at sikre, at dit hjemmenetværk er sikkert, er det vigtigt at have en stærk adgangskode til dit Wi-Fi-netværk. Dette gør det markant sværere for uvedkommende i at få adgang til dit netværk og dine personlige oplysninger. Derudover bør du ændre standardlogin og adgangskode til din router, da disse nogle gange kan være konfigureret med et standard loginnavn og adgangskode, såsom "admin”/”admin". Vælg et unikt og komplekst brugernavn og adgangskode for din router for at beskytte den mod uautoriseret adgang og ændringer af dine netværksindstillinger. Gå tilbage til afsnittet om adgangskoder, hvis du er tvivl om hvad en god adgangskode er.
På denne måde kan du opretholde et sikkert hjemmenetværk og beskytte dine enheder og data mod potentielle trusler.