DIGITAL ADFÆRD

Digital adfærd under kompetenceområdet
digital myndiggørelse

GRUNDEJERNES INVESTERINGSFOND

CIU Center for it i undervisningen

TEKNOLOGISK INSTITUT

Digital adfærd

Læsemål: Sikkerhed og Adfærd

I dette hæfte skal du lære om:

Digital adfærd · Netetik · Hvordan beskytter du dig på nettet?

Både som privatperson og som medarbejder behandler du data hver eneste dag. For dig som ansat i en virksomhed er der med indførelsen af GDPR den 18. maj 2018 blevet strammet op omkring, hvordan du skal håndtere data.

Derfor skal vi i dette kapitel bl.a. arbejde med emner som:
Informationsspredning - god adfærd i digital kommunikation

MENNESKELIGE FEJL

Du og dine klassekammerater ved selvfølgelig godt at i skal passe på jeres personlige oplysninger og at man skal træde varsomt i den digitale verden. Alligevel viser flere undersøgelser, at 25% af brud på IT-sikkerheden sker på grund af menneskelige fejl. Vi skal altså alle være med til at beskytte os selv og virksomhedens data.

Men hvordan passer man på sig selv i den digitale verden? Du kan starte med at holde dig opdateret om teknologi og trusler. Og så kan du bevidst arbejde med din adfærd på nettet og de sociale medier. Hvis du også sørger for at uvedkommende ikke kan få adgang til dine data og devices, er du nået langt.

DISKUSSIONSOPGAVE OM IT SIKKERHED

Overvej hvordan i passer på jeres data i den digitale verden?

VIDEN

Jo mere du ved om IT sikkerhed, jo bedre. Du skal kende til trusler som virus, phishing og hvordan du laver en sikker adgangskode for at være et skridt foran. På din arbejdsplads har du et medansvar ift ikke at lukke uvedkommende ind i systemerne.

ADFÆRD

Du kan selv gøre meget for at undgå problemer. Ved at opføre dig fornuftigt og bruge din viden bliver du et skridt foran IT kriminelle. Her følger nogle gode råd:

GODE RÅD OM ADFÆRD

- Brug din sunde fornuft, når du surfer
- Vær kritisk over for de kilder du finder
- Tænk dig om når du deler noget på de sociale medier
- Opdater din computer og dine programmer (også apps), så der ikke opstår huller
- Brug din computers indbyggede firewall
- Lav gode og stærke password
- Undlad at bruge det samme password alle steder
- Skriv ikke dine password ned
- Tag jævnligt en sikkerhedskopi af dine data
- Tænk dig om, når du bruger usikrede eller offentlige netværk

Sikkert netværk PowerPoint
Sikkert netværk video

ADGANG

Pas på din elektronik og sørg for at andre ikke kan få fysisk adgang til dine devices. Skulle du alligevel få stjålet din pc eller mobil, så hjælper det, hvis de er beskyttet med sikre adgangskoder og biometriske data.

Kryptér også indholdet på dine elektroniske devices, så andre ikke kan læse indholdet. Selvom din pc er beskyttet med adgangskode, kan en IT-kriminel tage harddisken ud af din pc og med lidt teknisk snilde læse indholdet alligevel.

Trusler fra nettet

Virus · Keylogger · Video: *Sådan undgår du phishing*
Øvelse: *Quiz om sikkerhed*

IT-sikkerhed er en af de største udfordringer ved brugen af informationsteknologien. Vores samfund og du som IT-bruger er utrolig sårbare overfor truslerne fra internettet. Du skal både passe på din egen IT sikkerhed, men du har også et stort medansvar ift. beskyttelse af virksomhedens.

Når du færdes på internettet, lurer mange farer. Inden du ser dig om, kan din computer være fyldt med malware som:

- Virus
- Trojansk hest
- Spyware
- Adware

Når du handler på nettet eller bruger din netbank, er der også en risiko for, at dine informationer bliver stjålet. Derfor er det vigtigt, at du opdaterer din PC og bruger din sunde fornuft.

I dette afsnit vil du lære mere om de forskellige farer, internettet rummer. Du vil også lære noget om, hvordan du bedst beskytter dig, når du surfer rundt på nettet.

ANTIVIRUSPROGRAM
Et program der forhindrer skadelig software i at komme ind på din pc / virksomhedens netværk. Beskyt din pc med et ordentligt antivirus program. Det kan fx være Windows Defender eller et program fra fx AVG, Symantec eller Norton.

VIRUS
En virus er et lille softwareprogram, der skjuler sig i andre programmer eller i vedhæftede filer. Virussen kan være programmeret med mange formål fx at kopiere sig selv til andre computere, uden at brugeren opdager det. En virus kan også indeholde en "trojansk hest", der åbner en "bagdør" på din PC, som gør det muligt at overtage eller fjernstyre din PC og få adgang til dine informationer.

En virus er lavet for at ødelægge og forstyrre din computers funktioner. Der er tre hovedgrunde til at udvikle vira:

- Tjene penge
- Stjæle informationer
- Genere andre

Det typiske er, at virussen bruger din e-mail eller til at sprede sig på andre computere. Men det kan også spredes igennem tjenester som Messenger, WhattsApp osv. Derfor kan en virus være skadelig både for din PC, men også for dine venner og andre kontaktpersoner.

ET VIRUSPROGRAM

- Arbejder i det skjulte og bruger hele tiden lidt af computerens processorkraft
- Er nogle gange bare til for at genere brugeren, mens den andre gange ødelægger vigtige filer på computeren Lægger sig ind i en anden software, da den kan ikke fungere alene

Når programmet eller styresystemet startes af brugeren, aktiveres virussen inden den rigtige software. På den måde starter og spreder virussen sig. De fleste vira er udviklet til at kopiere sig selv et bestemt antal gange, før dens skadelige virkninger viser sig.

ORM

En orm er en skadelig software, som flytter sig fra computer til computer i et netværk, uden at den skal aktiveres ligesom virussen.

Orme udnytter svagheder i styresystemet eller web-browseren i virksomhedens netværk, og har ofte skadelige programmer med som en trojansk hest eller en virus. Nogle orme kan misbruge mailprogrammets adressebog og videresende sig selv til kontaktpersonerne i adressebogen.

TROJANSK HEST

En trojansk hest er et ondsindet software, som er forklædt som et nyttigt program fx en falsk sikkerhedsopdatering.

Orme udnytter svagheder i styresystemet eller web-browseren i virksomhedens netværk, og har ofte skadelige programmer med som en trojansk hest eller en virus. Nogle orme kan misbruge mailprogrammets adressebog og videresende sig selv til kontaktpersonerne i adressebogen.

KEYLOGGER

En keylogger er en software, der registrerer alt input fra tastaturet.

Det bruges til at udspionere din pc, oftest med henblik på at stjæle passwords, kontonumre og andre følsomme oplysninger, når du handler eller ordner bankforretninger via nettet.

SPYWARE

Spyware eller spionprogrammer er programmer, der installeres på en computer, som regel uden at brugeren ved noget om dette.

Spyware er små spionprogrammer, der indsamler informationer om:

- Dine interesser
- Din adfærd
- Dine vaner på internettet.

De kan også samle informationer fra din harddisk og på den måde få adgang til informationer om netbank, dine kortoplysninger og passwords, som du bruger til forskellige tjenester på internettet.

Spyware sender informationer til de bagmænd, som har udviklet programmerne. De kan bruge oplysningerne til økonomisk kriminalitet, eller de kan sælge oplysningerne videre, så de fx kan bruges til målrettede reklamer. Spyware er altså en form for overvågning af dig og din brug af IT. Spyware installeres ofte sammen med et andet program, som vi downloader fra internettet. Måske står der faktisk i betingelserne, at der installeres spyware. Men hvem læser de ofte lange og uforståelige betingelser forud for download?

Spyware og adware fortjener ikke helt at blive kaldt vira, men de er irriterende og kan være skadelige for dig.

Man kan beskytte sin computer mod spyware, men ligesom antivirusprogrammerne skal disse opdateres tit for at kunne følge med udviklingen. Spyware udspionerer dig ligesom en keylogger.

ADWARE

Adware er et program, der er udviklet til at vise reklamer på din computer, omdirigere dine søgninger til websteder fyldt med reklamer og indsamle markedsføringsoplysninger om dig.

Adware er mere harmløse programmer, da de ikke sender informationer tilbage til bagmændene. Adware kan:

- Vise sig som pop-up vinduer med reklamer
- Ændre indstillinger i browseren fx startsiden
- Installere uønskede søgemenuer
- Tilføje bookmarks i browseren

Alt sammen meget irriterende og forstyrrende, når du skal arbejde på din PC. Adware installeres på samme måde som spyware, når vi downloader et program eller spil fra internettet.

De fleste malware ødelægger ikke computeren rigtigt, men gør den langsommere. De er er lavet for at indsamle informationer om dig. Disse oplysninger kan fx bruges til at sende målrettede reklamer. Reklamerne vises typisk i form af e-mails, hjemmesider der åbner automatisk, eller pop-up beskeder.

PHISHING

Phishing betyder, at IT-kriminelle "fisker" efter dine private oplysninger.

Ofte bruges falske e-mails, beskeder på Facebook eller Twitter, der forsøger at få dig til at afgive personlige informationer fx brugernavn, adgangskode, kreditkorts- eller netbank oplysninger.

Beskederne eller e-mails kommer angiveligt fra personer du kender, fx fra din bank eller offentlige myndigheder som SKAT. Umiddelbart ser det meget rigtigt og officielt ud, men det er vigtigt, at du er opmærksom og læser beskeden grundigt igennem, inden du afgiver oplysninger. Og som regel beder disse organisationer aldrig om gen sendelse af dine oplysninger.

Tidligere var det lettere at genkende phishing mails, da de var skrevet på dårligt dansk. I dag er de it-kriminelle blevet mere professionelle, og det kan til tider være svært at spotte svindlerne. Men der er dog stadig kendetegn, der kan hjælpe dig til at identificere phishing.

Se video først i materialet fra Jydske bank

PHISHING

Spam er mails med reklamer, som man ikke selv har bedt om at få.

Hvis du modtager e-mails, der reklamerer for fup-kontaktannoncer, porno, vækshormoner, Viagra osv., er det spam.

Spam er altså e-mails, som masseudsendes for at reklamere for fx produkter. I 2013 anslog IT-sikkerhedsfirmaet Kaspersky Lab, at 70-75% af alle sendte e-mails er spam.

I Danmark er det forbudt at udsende spam, derfor beder virksomheder på nettet dig ofte om, om du vil modtage deres nyhedsbrev.

I Danmark er spam-mails omfattet af Markedsføringsloven §6a, som i korte træk forbyder en virksomhed at tage uopfordret kontakt til nogen med en kommerciel hensigt. Paragraffen omfatter elektronisk post, telefax og automatiske opkaldssystemer.

Øvelse: Quiz om sikkerhed

Quizzen laves som Kahoot på klassen

Cookies på nettet

Cookies · Ja tak til cookies

COOKIES

En cookie er en fil, der gemmes på din computer, tablet eller smartphone, når du besøger en hjemmeside.

Når du surfer på nettet, lægger varer i en indkøbskurv eller indtaster oplysninger på en hjemmeside, kan disse informationer blive gemt på din PC i en tekstfil - en såkaldt cookie. Næste gang du besøger hjemmesiden, husker den dine valg og gør det nemmere for dig, fx ligger dine varer stadig i indkøbskurven.

En cookie kan ikke se, hvem du er, hvad du hedder, hvor du bor, eller om computeren bruges af en eller flere personer. Den kan heller ikke sprede computervirus eller andre skadelige programmer. Der findes forskellige cookies, og de har forskellige funktioner.

HJÆLPE COOKIES

Hjælper din PC med at huske forskellige informationer på en hjemmeside fx dit password, indholdet i din indkøbskurv eller opsætningen på en hjemmeside.

En hjælpe cookie gemmes på din PC og udløber efter en given tid. Fx kan indkøbskurven på en webshop huskes i 5 dage, mens din opsætning på dr.dk's tv-oversigt huskes meget længere.

SESSIONS COOKIES

Skriver løbende i cookie filen, mens du besøger hjemmesiden. Den bruges til at genkende dig, når du bevæger dig rundt på siden, fx om du er logget ind. En session cookie slettes, når du lukker browseren ned.

TRACKING COOKIES

Er farlige, da de kan sende oplysninger om din færden på internettet til andre personer. De kan kodes på en ret avanceret måde, og derved gøre det muligt for andre at udnytte den viden, de får om dig.

TREDJE PARTS COOKIE

Bliver gemt på din computer af et andet websted end det, du besøger. Disse tredjeparts-cookies bruges bl.a. til målrettet markedsføring i bannerreklamer og til at vise irriterende pop-up reklamer på din skærm.

JA TAK TIL COOKIES

I december 2011 indførte Erhvervsstyrelsen en cookie lov, den såkaldte cookie-bekendtgørelse. Den stiller krav om, at virksomheder skal oplyse dig om, hvilke cookies der gemmes på din pc, hvis du bevæger dig rundt på deres hjemmeside.

Du skal selv give virksomhederne lov til at gemme cookies - derfor bliver du bedt om at acceptere cookies. Desværre oplever de fleste af os det som irriterende og forstyrrende. Vi klikker bare på "*Ja, jeg accepterer cookies*" uden helt at sætte os ind i, hvad vi siger ja til.

Netetik/kildekritik

Kildekritik · Hvordan er man kildekritisk? · Kildekritiske spørgsmål

RO PÅ

Mange online scams bygger på at der skabes et element af panik. Du skal gøre noget her og NU! Det er fordi at den der prøver at narre dig gerne vil have at du ikke er alt for kritisk ift de fantastiske tilbud han tilbyder dig. Eller måske er det din 'bank' der skriver at du skal skynde dig og sende nogle oplysninger da de vil tjekke dine oplysninger?

Ro på. I den digitale verden er det fornuftigt at holde hoved koldt og tænke sig om 2 gange. Og er du tvivl, så spørg en kollega, familiemedlem eller kammerat til råds. Så snart 2 par øjne har set på det, så ser tingene ofte anderledes ud.

KILDEKRITIK

Kildekritik handler om hele tiden at forholde sig kritisk til sine kilder. Man skal både være kritisk overfor, hvad kilden fortæller en, hvem afsenderen er, og hvad formålet med kilden kan være.

I alle sammenhænge, hvor du anvender kilder til at finde informationer, er kildekritik vigtigt. Det er særlig vigtigt at være på vagt overfor materialer fundet på nettet, da alle i princippet kan lægge hvad som helst ud på nettet. Det betyder, at meget af indholdet på internettet kan være af tvivlsom kvalitet. Det er dit ansvar at sikre, at den information, du fx bruger i en opgave, er troværdig og aktuel.

Internettet er det første sted, vi leder, når vi vil vide mere om et emne. Det er det først og fremmest, fordi det er langt hurtigere at gå på nettet end at gå på biblioteket.

HVORDAN ER MAN KILDEKRITISK?

Hvordan afgør man, om en webside er troværdig? Og hvordan gennemskuer man, om den information, man finder, er brugbar?

1. Tjek hjemmesidens adresse

Hjemmesidens URL kan ofte sige noget om troværdigheden af en side. Fx er en side under denstoredanske.dk mere troværdig end en hjemmeside, der starter med 123hjemmeside.

Når du søger på Google, bliver du ofte henvist til en underside eller artikel om emnet. Sørg for at finde tilbage til hovedsiden, så du kan finde ud af, hvilken institution, virksomhed, organisation eller person, der står bag siden.

2. Hvem er afsenderen, og hvad er formålet med siden?

Undersøg hvem afsenderen er. Ofte kan du finde en side, der hedder "Om ..." Her kan du læse, hvem afsenderen er, og hvad formålet for siden er. Hvis ikke du kan finde informationer om afsenderen, skal du være ekstra kritisk.

3. Kontaktmuligheder

Er der mulighed for at kontakte afsenderen eller ejeren af hjemmesiden? Hvis muligheden ikke findes på siden, skal du igen vurdere, om hjemmesiden er troværdig.

4. Se på sammenhængen

Indeholder hjemmesiden synspunkter, informationer eller billeder, der virker til at være uden for sammenhængen? Gives der udtryk for skarpe holdninger, eller er der mange politiske ytringer? Og hvordan er sprogbrugen?

5. Er siden aktuel?

Internettet er fyldt med forældet information. Tjek om du kan se, hvornår siden sidst er blevet opdateret - og hvornår siden er oprettet. Husk at videnskabelige eller historiske artikler ikke nødvendigvis er forældede, fordi de er gamle. Nyhedsartikler mister derimod hurtigt relevans og aktualitet.

6. Krydstjek med andre kilder

For at sikre at den information, du har fundet, er korrekt, er det en god idé at krydstjekke med andre kilder. Det kan både være via andre hjemmesider, men også gerne andre kildetyper. Fx kan du gå en tur på biblioteket.

KILDEKRITISKE SPØRGSMÅL

Her finder du en liste over gode kildekritiske spørgsmål, som du kan stille, når du skal vurdere en hjemmeside: biblioteket.

- Fremgår det tydeligt, hvem der har skrevet indholdet?
- Er vedkommende kvalificeret til at skrive om emnet?
- Fremgår det tydeligt, hvornår siden er oprettet?
- Er siden objektiv dvs. uden stærke holdninger og meningstilkendegivelser?
- Er siden fri for klare politiske, ideologiske eller kommercielle tilhørsforhold?
- Går siden i dybden med emnet?
- Bidrager siden med relevante oplysninger i forhold til dine andre kilder?
- Er sidens links kommenterede, og er de relevante i forhold til dens indhold?

Hvordan beskytter du dig på nettet

Forebyggelse fremfor helbredelse · Videoer fra Netsikker nu! med Krysters Kartel
Sådan laver du et sikkert password PowerPoint · Biometriske data
Øvelse: Tjek dit password

FOREBYGGELSE FREMFOR HELBREDELSE

Det er lettere at forebygge end at helbrede. Det gælder også, når vi snakker computere. Det er lettere at sørge for at beskytte din computer og dig selv mod virus, spyware, adware, spam og phisning, end at fixe det senere, når skaden er sket.

Du kan selv gøre meget for at undgå problemer:

- Brug din sunde fornuft, når du surfer
- Opdater din computer og dine programmer, så der ikke opstår huller
- Brug din computers indbyggede firewall
- Lav gode og stærke password
- Undlad at bruge det samme password alle steder
- Skriv ikke dine password ned
- Tag jævnligt en sikkerhedskopi af dine data
- Tænk dig om, når du bruger usikrede eller offentlige netværk

Videoer fra netsikker nu! Med Krysters Kartel

- Netsikker nu! Facebook og indbrud
- Netsikker nu! porno og virus
- Netsikker nu! Svindel

SÅDAN LAVER DU ET SIKKERT PASSWORD

Se PowerPoint omkring password

Undgå at bruge de typiske ord til password fx børnenes, hundens eller kærestens navn eller fødselsdato. Brug heller ikke de typiske talkombinationer fx 0000 eller 1234 - eller gennemskuelige ord som hemmelig, secret eller andre ord, som er nemme at gætte.

Lav lange kodeord

Kodeord som består af 8 tegn eller mere er svære at bryde. Hackere er gode til at bryde passwords.

Hvis du kun bruger små bogstaver i dit kodeord:

- Vil et password på tre tegn tage 0,02 sekund at bryde
- Otte små bogstaver, vil tage 2,4 dage for en computer at bryde
- Kan du finde et kodeord på 11 små bogstaver, vil det tage en computer omkring 116 år at bryde din kode.

Brug både tegn, tal og store bogstaver

Jo flere kombinationsmuligheder du bruger, jo bedre. En kombination af tal, tegn og bogstaver på 11 karakterer vil tage en computer op til 180.365.000 år at bryde.

Erstat fx bogstaver med tal eller tegn fx o med 0, a med @, l med 1, g med 9 eller lignende.

Hvis du vil bruge alligator som password, kunne det se sådan ud, når du bytter rundt på tegn, tal og bogstaver: @119@t0r

Det er et godt password, som er svært at bryde.

Øvelse: Tjek dit password

Du har lige læst om sikre passwords, herunder hvordan du laver et password, der er svært at bryde.

Du skal nu teste dit password på Kapersky Labs hjemmeside. Kaspersky Lab er en virksomhed, der arbejder med computersikkerhed. De udvikler og sælger programmer, der beskytter mod virus, spyware, spam

- Brug Check your password og tjek dit nuværende password
- Hvad er dommen over dit password? Er det godt eller skidt?
- Hvor ofte findes det i databaser med lækkede passwords?
- Hvor lang tid tager det at knække dit password med en almindelig pc?
- Hvad skal du gøre for at lave et sikkert password?
- Prøv nogle nye passwords af.