



Cyber Safety

Protecting yourself in the digital age

Starting Soon



Cyber Safety

Protecting yourself in the digital age

Outline



1. Use cases
2. Common scams
 - Email
 - SMS - Guest Speaker: Umesh Giri
 - Voice
3. Online shopping
4. Invoice fraud - Example: Jeevan Thapa
5. Facebook Marketplace
6. Used bike/cycle
7. Marketplace and DBA Shopping Risks and mitigations
8. Facebook common security issues
 - Account Takeover - Guest Speaker: Laxman Kandel
 - Phishing and scams
 - Identity theft
 - Unwanted tagging
9. Enable 2-Factor Authentication in Facebook
10. General Awareness

Use Cases

1. Facebook Marketplace, DBA
2. Facebook group - Nepali Living in Denmark
3. Stolen Bike, mobile, etc?
 - a. Check serial number in Politi if receipt is not provided
4. When making payment from mobile pay, take a picture and put it under remarks
5. Fake Rental Contract
6. Be careful while clicking in any link provided in the social media

Common scams

1. Through Email
2. Through SMS
3. Through Phone Call

Email scams

1. Disguise as Danish authorities or organization
2. Disguise as a genuine organization/company

Example 1:



Fra: "mitid.dk" <support@adwardando.co>
Dato: 25. juli 2023 kl. 08.27.00 CEST
Til: [REDACTED]
Emne: **Vigtig meddelelse, læs omhyggeligt**



Kære borger,

Vi ønsker at informere dig om en vigtig ændring vedrørende adgangen til digitale tjenester. Som du måske allerede er bekendt med, benytter du i øjeblikket NemID til forskellige online handlinger. Vi vil gerne gøre opmærksom på, at for at sikre en mere moderne og sikker adgang til digitale tjenester er det nødvendigt, at du skifter fra NemID til MitID inden for de næste 24 timer.

Vi opfordrer dig til at handle hurtigt for at undgå afbrydelse af din digitale adgang. Tøv ikke med at tage kontakt til os, hvis du har yderligere spørgsmål eller bekymringer.

Med venlig hilsen,

Danish Authority for Digitisation

[Blive ved](#)

Example 2:



Opdatering påkrævet: Ny anmodning om enhedsadgang Inbox x

 **MitiDDigst DK** <noreply@campaign.eventbrite.com>
to me ▾

Vi kontakter dig for at informere dig om, at der er registreret en ny enhed, der forsøger at få adgang til din konto. For at sikre sikkerheden af dine oplysninger kræver vi din øjeblikkelige opmærksomhed.

For din sikkerhed skal du følge nedenstående trin for at opdatere din adgangskode:

1. Log ind på din MitiR ved hjælp af linket nedenfor.
2. Naviger til "Enhedsåndtering".
3. Vælg "Skift adgangskode" eller lignende mulighed.
4. Følg vejledningen for at oprette en ny, sikker adgangskode.

Hvis du mener, at dette adgangsforsøg var uautoriseret, bedes du straks kontakte vores supportteam.

[Fortsæt ->](#)

Tak for din opmærksomhed på denne sag.

Med venlig hilsen,

MitiRDigst DK



MitiDDigst DK
Sygehusvej 241, Kolding, Kolding 6000 DK
[Unsubscribe](#) | [Privacy Policy](#)

Example 3:

From: Microsoft OneDrive <onedrive@electric-utilities.co.uk>
Subject: Your OneDrive is almost full.

Impersonation
Attackers will mask the sender's e-mail address to appear legit, so always hover over to check the original e-mail. They must match.

Microsoft OneDrive

OneDrive storage is almost full

Relevance?
When receiving an e-mail consider why you received it. Use common sense to determine whether it is relevant for you or not, and whether it makes sense.

Your jos@secureddevice.dk OneDrive storage is almost full. When your OneDrive storage is full, documents, pictures, and edits will not synchronize with OneDrive.com or your devices. Additionally, you won't be able to add new documents and pictures.

To continue using OneDrive, you need to [upgrade your storage](#) or [remove files](#) you no longer need.

Unusual request
The attackers want information from you, so they will try to get you to enter your credentials or give access to applications.

Suspicious links
Malicious links are often long, contain unexpected words or is inconsistent to where it is supposed to send you.

Always be wary of requests with links.

[Buy more storage](#)

Always check before you click.

This email was sent from an unmonitored mailbox.

You are receiving this email because you have a Microsoft OneDrive account.
[Privacy Policy.](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 USA

Microsoft

How to avoid/prevent?

1. Report the email as a phish and DELETE it.
2. If got phished, report it as soon as possible.

DON'T PANIC!

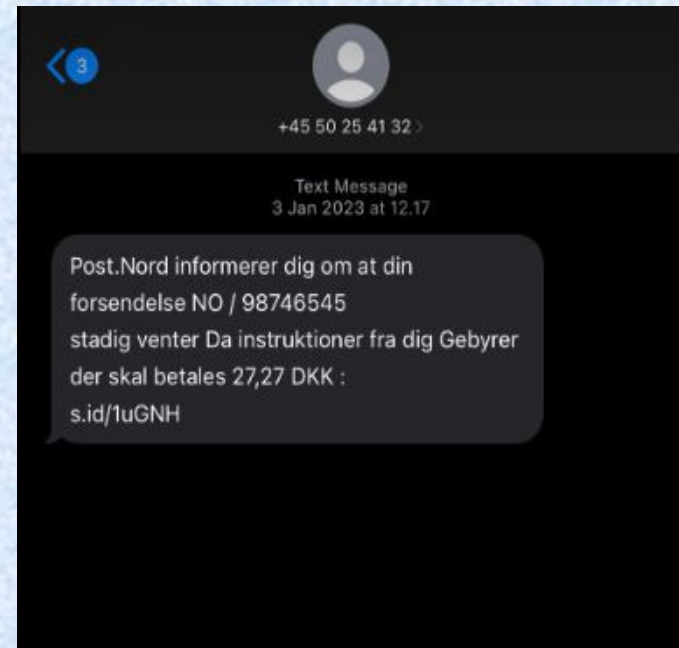
Prevention is important but reaction is even more important!

- a. Have your payment card or MitID blocked?
 - b. Contact your bank to stop the transfer.
3. If there has been abuse, report it via politi.dk

SMS scams

1. Package Deliver
2. Refund Claim
3. Danish Authorities

Example 1: Regarding a package /delivery



Example 2: To update personal information



Example 3: Regarding Refund



How to avoid/prevent?

1. **DELETE the SMS/text message.**
2. If got phished, report it as soon as possible.

DON'T PANIC!

Prevention is important but reaction is even more important!

- a. Have your payment card or MitID blocked?
 - b. Contact your bank to stop the transfer.
3. If there has been abuse, report it via politi.dk



Example from guest speaker:

Umesh Giri

Voice scams

1. To promote marketing
2. Danish organization or authorities: SIRI, MitID, Police
3. Microsoft
4. Threat calls

Voice call scams

1. Danish police warn of scam phone calls from fake officers
2. Foreigners in Denmark targeted by phone scammers

**National enhed for Særlig Kriminalitet (NSK)**
@NSK_politi · [Follow](#)



BE AWARE OF TELEPHONE FRAUD 

Criminals claiming to be from the police or other governmental authorities are now targeting foreigners living in Denmark in an attempt to persuade them to provide personal information or bank details [#politidk](#) [#nsk](#)

JUST HANG UP
- and other tips on avoiding fraud

Be wary of any calls, texts or emails asking for your personal or financial details, or for you to transfer money

Just hang up the phone - it's better to be safe than sorry

In doubt? Call your bank, the police (on 114) or a friend

POLITI

10:02 AM · Aug 1, 2023 

 52  Reply  Share

[Read 6 replies](#)



How to avoid/prevent?

1. Never give out personal/sensitive information.

HANG UP THE PHONE !

2. If got phished, report it as soon as possible.

DON'T PANIC!

Prevention is important but reaction is even more important!

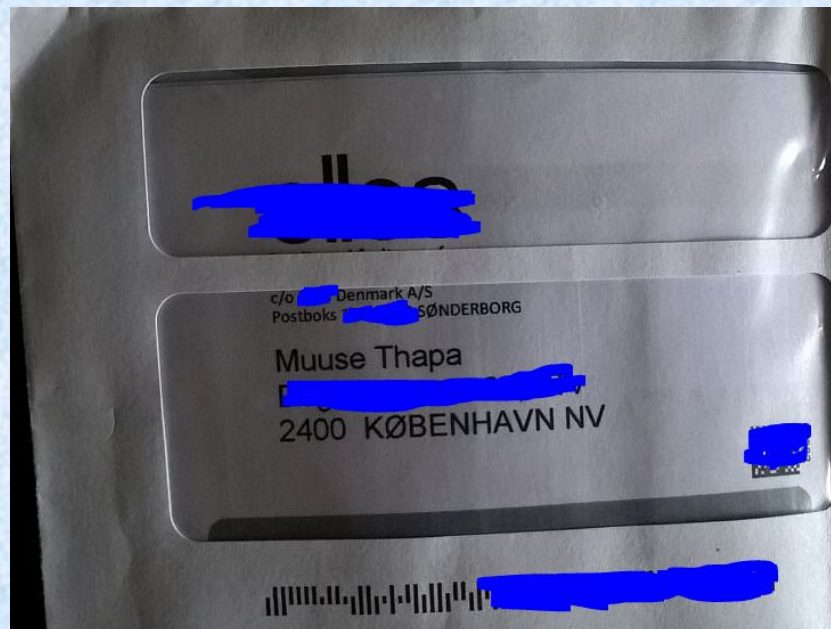
- a. Have your payment card or MitID blocked?
- b. Contact your bank to stop the transfer.
- c. Hide details from public - contact the provider.

3. If there has been abuse, report it via politi.dk

Online Shopping

1. Careful when using debit/credit cards
2. Use of Apple pay or Mobile pay, if the option is available
3. Report on online purchase issue

Case from Jivan Thapa Magar



CPR Misuse

Online Shopping:

Buy now / Pay later

CPR Number

3. Betalingsmetoder

☐ Betalingskort - MobilePay - Viabill



☐  Betal i 3 dele

☐  Køb nu. Betal senere.

☐  Betal nu



Case from: Invoice fraud

Report to police

Via email with details

<https://politi.dk/en/crimes-against-digital-devices>



Break

Facebook: Marketplace phishing



Product is listed on marketplace

Contact address with real company address in Denmark

Price is realistic with 10-20% off, so hard to notice

Webshop: Apple iPad Pro 11.0" (2022) 128GB - Space Grey 7.999,00 kr.

Spammer Market place/DBA : Apple iPad Pro 11.0" (2022) 128GB - Space Grey 5.999,00 kr.

Payment: Pay by Bank and Pickup

Pretending to be a sales person from the company

Scammer disguise as a real company employee and ask for payment pay via bank transfer, and pickup later at the real company location

- Hard to identify, it is a scam

Facebook: Marketplace stolen items



Mobile

Laptop

!!! cycle (bike)

- **Ask bike serial number of bike / cycle**
- **Check serial number on the Police website / politi site**

Ask for invoice

Ask for written document that you made a purchase if they do not have original receipt

Facebook: Marketplace

1. Check the user profile
2. Never pay by Bank Transfer, use Mobile Pay instead
3. Avoid delivering goods via delivery service
4. Save the chat history

Used bike / cycle

<https://politi.dk/cykler-og-koeretoer/tjek-om-en-cykel-eller-et-koeretoer-er-efterlyst/tjek-om-en-cykel-er-efterlyst>

POLITI

Forside / Service og tilladelser / Cykler og køretøjer / Tjek, om en cykel eller et køretøj er efterlyst
/ **Tjek, om en cykel er efterlyst**

Tjek, om en cykel er efterlyst

Indtast cyklens stelnummer og se, om den er meldt stjålet i politiets cykelregister. Det kan være nyttigt, hvis du fx vil købe en brugt cykel eller kender til en efterladt cykel.

Vær opmærksom på, at politiets cykelregister kun registrerer danske cykelstelnumre og cykelstelnumre på max 19 karakterer. Det er derfor ikke muligt at tjekke, om cykler med længere stelnumre er efterlyst af politiet.

Hvis du har købt en cykel i/fra udlandet, kan du få udleveret et politistelnummer ved henvendelse på en politistation. Husk at rette telefonisk henvendelse til politistationen først for at sikre dig, at du kan få stelnummeret på den pågældende politistation. Læs mere om [cykler købt i udlandet](#).

Tjek, om en cykel er efterlyst af politiet

Indtast cyklens stelnummer

☐

I'm not a robot

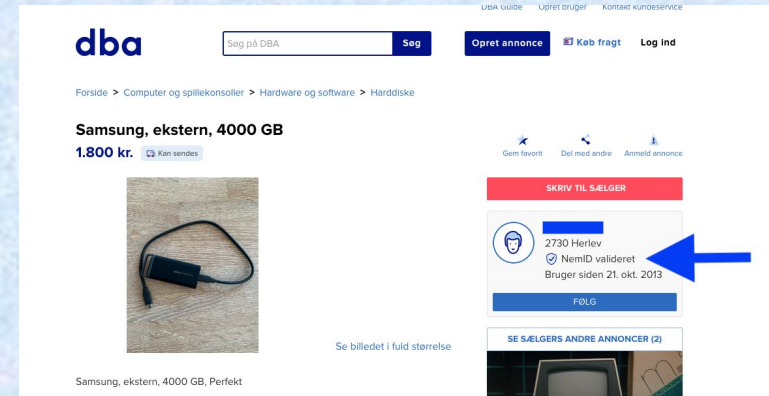


Privacy - Terms

Marketplace and DBA Shopping Risks and Mitigations



1. Always screenshot the listing and save it in secure place(email yourself)
2. Ask for invoice bill
3. Cross - check if the item same as listing.
4. Pay via mobile pay avoid paying in cash
5. In case of DBA choose the seller with nemID/MITID verified.



Facebook common security issues, mitigations

1. Account Takeover(ATO)



Issues	Mitigations
Unauthorized individuals gaining access to user accounts • phishing attacks, • password guessing, • exploiting vulnerabilities	• 2FA (Two Factors Authentication) • Unique and strong passwords • Avoid easy to guess words like (name,DOB,phonenumber,"123456789","qwerty","abc123","letmein","password1","admin","welcome","123abc","iloveyou","football","123123","monkey" etc) • Use combination of special characters like &,#,!,numbers,alphabetes (got.Hello@201)

Example from guest speaker:



Laxman Kandel



Facebook common security issues, mitigations

2. Phishing and Scams



Issues	Mitigations
Users falling victim to • phishing emails, fake pages, • scams aiming to steal login credentials or personal information  A screenshot of a news article from the Danish newspaper B.T. The headline reads 'Beskyldningerne mod Divya Das er blevet bekræftet' (The accusations against Divya Das have been confirmed). The article features a photo of a woman, Divya Das, being interviewed by a news outlet (TV2). The text below the photo mentions that she appeared on Danish TV in connection with a tragedy and that she held her wedding over the weekend. WWW.BT.DK Divya Das optræden på dansk tv i går endte i en tragedie. Kim Bildsøe Lassen og Divya Das holdt i weekenden deres bryllup - igen Læs mere	• Identify fake pages - Surf secure pages (starts with https) - Avoid pages (starts with only http) - Prefer for web pages end with .dk • Unique and strong passwords

Facebook common security issues, mitigations

3. Identity Theft



Issues	Mitigations
Use of user identities for malicious activities • creating fake accounts or • conducting scams. A screenshot of a Facebook search results page for the name 'Elon Musk'. It displays a list of six profiles, all of which are fake. Each profile has a small circular profile picture and a name that is a variation of 'Elon Musk'. The first profile is 'James Arthur (Elon Musk)' with the bio 'Manager at United State Marines · 1 follower'. The second is 'Elon Reeve Musk' with 'Works at Tesla · Pennsylvania · Lives in Usa'. The third is 'Elon R Musk' with 'Lives in Baltimore, Maryland'. The fourth is 'Elon Reeve Musk'. The fifth is 'Elon Musi (Elon musk)' with 'Works at Space x C.E.O and architect of Tesla High School (St. Paul, Minnesota) · Lives in Ne'. The sixth is 'Elon Reeve Musk' with 'Lives in Houston, Texas'. The last profile has a black profile picture with a white 'X'.	• Try to make your personal information public as less as you can. • Report suspicious activity

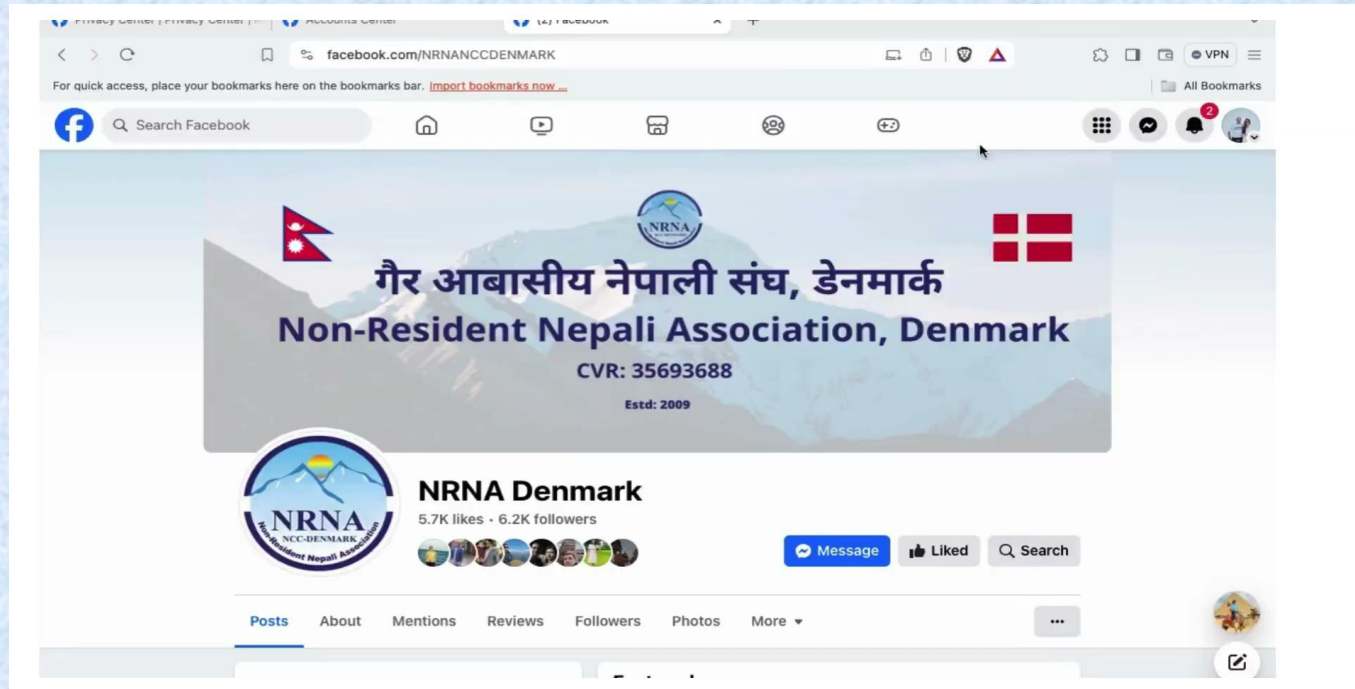
Facebook common security issues, mitigations

3. Unwanted Tagging



Issues	Mitigations
Tagged in unwanted post • Friends tag to a post which you do not want. • Tagging without permissions	• Enable privacy policy for tagging • Report suspicious activity

Enable 2 factor authentication in Facebook



<https://nrna.dk>

General Awareness



1. Sharing of personal information via social media: CPR, phone number, bank info.
2. Enable 2 or multi factor authentication
3. Connect to secure Wi-Fi only
4. Precautions when logging in from others device
5. Pendrive/usb sticks found should not be used.
6. Stolen Bike, mobile, etc?
 - a. Check serial number in Politi if receipt is not provided
7. Be careful while clicking in any link provided in the social media.



Questions ??



Quiz Time



Thank You !