# HÖJ DIN SÄKERHET ONLINE

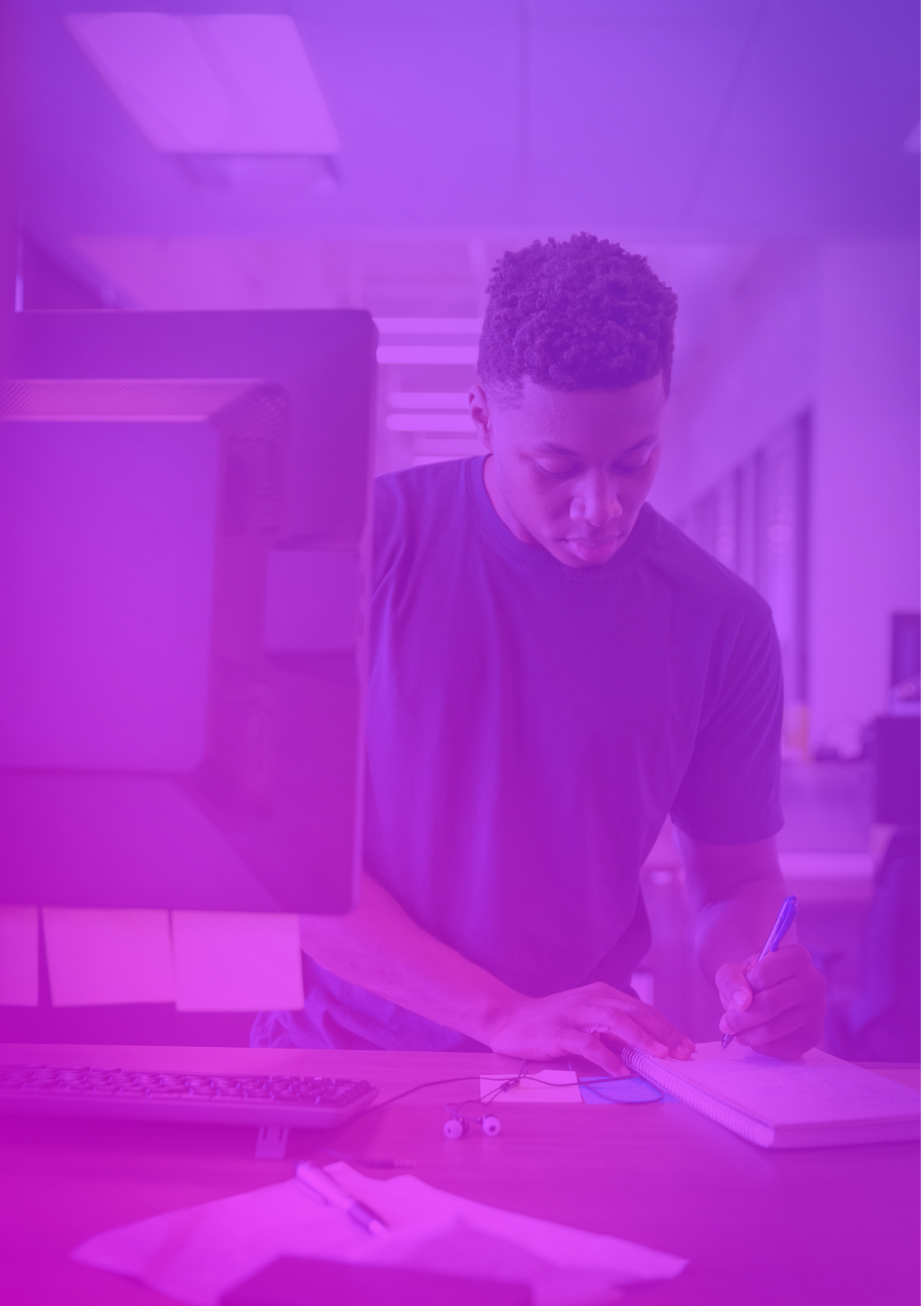
## HANDFASTA TIPS FÖR ATT SÄKRA UPP DIN VERKSAMHET

RAPPORTEN BESTÄLLD AV
tillväxtverket
Region Östergötland
LINKÖPING SCIENCE PARK

# DEL 1

## Grundläggande IT-säkerhet

*Ta del av konkreta tips för att plocka de lägst hängande frukterna för att säkra upp din uppkopplade verksamhet.*



# Minimum för en säker digital verksamhet

- Skapa starka och unika lösenord till dina olika konton
- Spara dina lösenord i en lösenordshanterare
- Aktivera 2-faktorsautentisering på alla konton där det är möjligt
- Håll alltid enheter uppdaterade
- Säkerhetskopiera viktig data

# Använd en lösenordshanterare

## Varför?

Använd nedan tips för lösenord till datorn, till lösenordshanteraren och övriga ställen där du måste memorera ett lösenord. För allt annat så bör du använda en lösenordshanterare. Det gör det möjligt att ha långa, komplexa och enskilda lösenord till olika konton utan att du behöver ha dem memorerade i huvudet.

Fokusera först och främst på organisationskritiska konton. Detta är viktigt eftersom du annars riskerar att ett enda lösenord på vift kan ge angripare tillgång även till andra inloggningar.

## Vilken?

Det finns många lösenordshanterare att välja på, vissa bättre än andra. En vi rekommenderar som ett säkert alternativ är Bitwarden. Du kommer långt på gratisvarianten. Du kan installera den både på din dator och mobil, vilket gör att du kan spara ditt lösenord på ena enheten och sedan sömlöst använda den på den andra.

## Skapa starka lösenord med egendomliga fraser

- **Exempel på starkt lösenord: *“Bertil kör alltid 4 elefanter.”***
- **Lätt att komma ihåg och svårt att knäcka!**
- **Svaga lösenord kan hackas på nolltid!**
- **Grundregeln är att längden är viktigare än komplexiteten. Bilda därför gärna en kort mening av udda sammansatta ord enligt ovan.**

# Aktivera 2-faktors-autentisering (2FA)

## Varför ska jag göra det?

2FA ger dig ett extra skydd så att cyberbrottslingar inte kan komma åt ditt konto även om de skulle komma över ditt lösenord. Gör du det på ditt Microsoft-konto så minskar riskerna för att en obehörig kommer åt dina lagrade uppgifter med hela 99,99%.

## Hur fungerar det?

2FA fungerar genom att be om ytterligare information för att bevisa din identitet. Du får till exempel en kod skickad till din telefon när du loggar in med en ny enhet eller ändrar inställningar som till exempel ditt lösenord.

## Var börjar jag?

Börja med att aktivera 2FA (också kallat MFA) för din epost och gör det sedan för alla dina viktiga konton och system som har stöd för det. Som regel får du logga in på din molntjänst och gå till inställningar för att aktivera det och där följa instruktionerna.

Som regel så kräver det en applikation som du har installerad på din dator eller telefon, så som exempelvis Microsoft Authenticator om du kör Microsoft Windows eller inbyggda Keychain om du kör Apples produkter.

# Håll dina enheter uppdaterade

Det här är ingen engångshandling. Se alltid till att alla enheter har de senaste uppdateringarna för att minska risken för cyberincidenter. På så sätt minskar du risken för att någon angripare utnyttjar olika hål som kan finnas.

Se alltid till att uppdatera på förfrågan. Var dock säker på att förfrågan kommer från rätt håll och att ingen försöker lura dig med falska rutor på en hemsida till exempel.

# Säkerhetskopiera viktig data

Det är lätt att förstå varför man vill vara försäkrad efter att huset brunnit ned. Säkerhetskopiering är en försäkring!

Genom att regelbundet säkerhetskopiera dina data kan din organisation fortsätta att fungera även om du drabbas av en cyberincident. Säkerhetskopiorna kan innefatta papperskopior, flyttbara medier eller säkerhetskopior till molnet.

Skydda dig från det värsta scenariot innan det händer!


# DEL 2

## Tänk proaktivt

***Är du redo för att höja säkerheten ytterligare i din verksamhet så följer här några ytterligare tips och rekommendationer som bygger vidare på de mest grundläggande kontrollerna.***

# Förbered inför en IT-incident

Även om det är viktigt att införa bra säkerhetskontroller finns det ingen perfekt säkerhet.

Alla organisationer löper risk att drabbas av en potentiell cyber-incident, så det är viktigt att du förbereder hur du kan svara på det och planerar återställning i händelse av att det skulle hända.

- **Identifiera kritisk information**
- **Gör en förteckning över dina viktigaste partners som du använder för att driva din organisation**
- **Säkerhetskopiera regelbundet viktig information**
- **Gör en incidentplan**

# Identifiera kritisk information

För ett register över viktiga uppgifter, såsom kontaktuppgifter, epost, kalendrar och andra väsentliga dokument. Identifiera vilka nyckelsystem och resurser som krävs för att verksamheten ska fungera.

Att ha resonerat om systemen och informationen är halva arbetet. Det väcker en förståelse för vad som kan hända om informationen blir otillgänglig eller kommer på villovägar.

# Gör en förteckning över dina viktigaste partners för att driva din organisation

Detta underlättar ditt agerande i händelse av en incident och gör det möjligt för dig att hålla din organisation aktiv i händelse av otillgängliga system. Se t.ex. till att ha kontaktnummer för leverantörer, nummer för IT-support osv. Detta bör vara lagrat på en plats du kommer åt även om det inte går att logga in på företagets egna eller molntjänster.

# Säkerhetskopiera viktig information regelbundet

Testa att säkerhetskopian fungerar för att se till att du kan återställa informationen då det behövs.

Enklast är att göra stickprov på viktiga dokument.

Är det backup i molnet? Är det något som inte backas upp dit som du behöver hantera själv? Och klarar leverantören att hantera återställning om ni drabbas av utpressningvirus som låser alla filerna?

# Gör en incidentplan

Förvara den på ett säkert sätt så att du kan använda den om din utrustning stjäls eller skadas av en cyberincident. Med andra ord är det bra om den finns tillgänglig även i fysisk form.

Finns några intressenter som behöver information omgående?

Behöver du rapportera om läckta personuppgifter (GDPR) till Integritetsmyndigheten?

Vilka manuella steg kan du använda i stället för vad du vanligen gör digitalt i olika system?

# DEL 3

## Informations- och applikationstips

*Ytterligare tips för dig i besöksnäringen som vill ha fler källor till bra information eller tips på säkra applikationer.*

# Rekommenderade tjänster

### Lösenordshanterare
- Bitwarden (primär rekommendation)
- 1password (alternativ rekommendation)
- Undvik: Keeper, Nordpass och numera Lastpass.

### E-posttjänster
- Undvik: alla e-posttjänster som inte stödjer 2FA

### Klientskydd för Windows
- Microsoft Defender
- F-Secure/With Secure
- Bitdefender (för företag)
- Undvik: AVG, Avast

### VPN-tjänst (om du ens behöver en)
- Mullvad
- Proton VPN
- Undvik: nästan allt.

### Kryptering
- Bitlocker för windowsmiljö, tillräckligt bra för det mesta.
- Veracrypt för vanlig lagring, mer än tillräckligt
- Cryptomator för molnlagring.

RAPPORTEN BESTÄLLD AV

tillväxt verket

Region Östergötland

LINKÖPING SCIENCE PARK