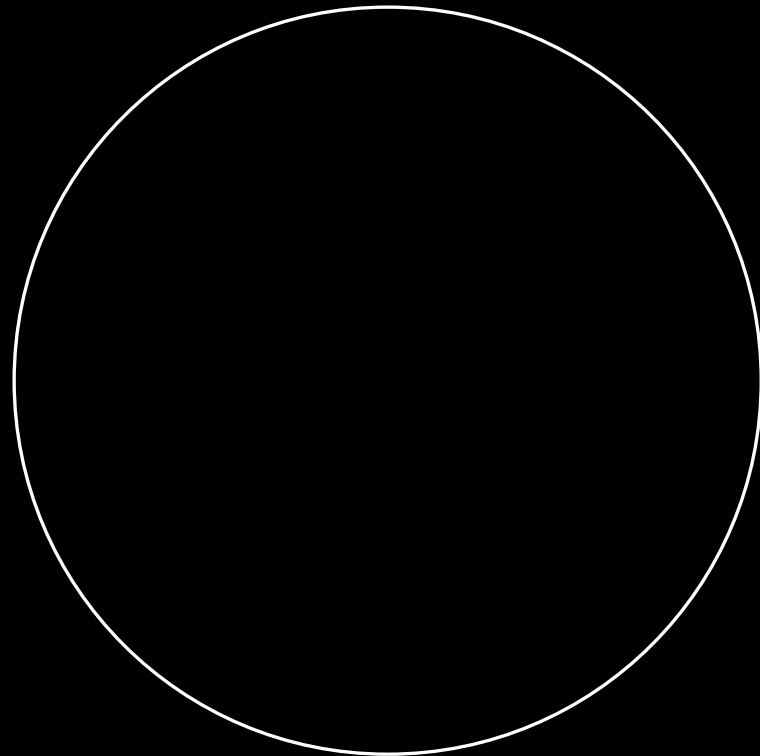


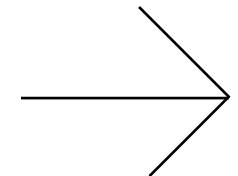
Utbildning i nätfiske för Axvalls IF:s styrelse

Förstå och skydda mot digitala bedrägerier effektivt

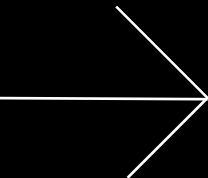


Utbildningens Agenda om Nätfiske

- Vad är nätfiske och varför drabbas idrottsföreningar?
- Så känner du igen nätfiske: vanliga metoder och varningssignaler
- Praktiska tips för att undvika nätfiske på dator
- Praktiska tips för att undvika nätfiske på mobiltelefon
- Vad gör man om man blivit utsatt för nätfiske?



Vad är nätfiske och varför
drabbas
idrottsföreningar?



Definition och syfte med nätfiske

Vad är nätfiske

Nätfiske innebär bedrägliga försök att lura användare att dela känslig information som lösenord eller betalningsuppgifter.

Syfte med nätfiske

Syftet med nätfiske är ofta ekonomisk vinning eller identitetsstöld genom att få tillgång till personlig information.

Varför idrottsföreningar kan vara särskilda mål

Ekonomisk hantering

Idrottsföreningar administrerar stora summor pengar, vilket gör dem sårbara för ekonomiska bedrägerier och missbruk.

Medlemsuppgifter

Hantera känsliga medlemsdata kräver skydd för integritet och förhindrande av identitetsstöld.

Samarbete med sponsorer

Sponsringsavtal och samverkan med externa parter kan utnyttjas av bedragare för ekonomisk vinning.

Exempel på konsekvenser vid lyckade attacker

Ekonomiska förluster

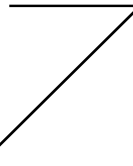
Nätfiske kan orsaka betydande ekonomiska förluster genom stulna pengar och bedrägerier.

Komprometterade medlemsdata

Personlig och känslig data kan bli exponerad och användas illvilligt efter en lyckad attack.

Skadat förtroende

Förtroendet mellan föreningen och dess partners kan minska kraftigt efter en nätfiskeattack.



Så känner du igen
nätfiske: vanliga metoder
och varningssignaler

Typiska kännetecken i e-post och sms

Brådskanie uppmaningar

Nätfiske använder ofta brådskanie meddelanden för att få mottagaren att agera snabbt utan eftertanke.

Stavfel och ovanliga avsändare

Ovanliga avsändare och stavfel i meddelanden är vanliga tecken på nätfiske och bedrägeri.

Oväntade länkar och bilagor

Meddelanden kan innehålla skadliga länkar eller bilagor som kan infektera datorer eller stjäla information.

Vanliga bluffmetoder: falska inloggningssidor och bilagor

Falska inloggningssidor

Bedragare skapar kopior av riktiga webbplatser för att lura användare att lämna sina inloggningsuppgifter.

Skadliga bilagor

Skadliga bilagor kan infektera datorer med virus eller trojaner när de öppnas av användaren.

Skillnader mellan legitim och falsk kommunikation

Korrekt språk och avsändare

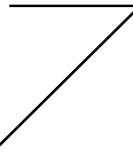
Legitim kommunikation använder korrekt språk och kommer från pålitliga och kända avsändare.

Säkra länkar

Säkra och betrodna länkar kännetecknar legitim kommunikation, vilket skyddar användare från bedrägerier.

Märkligheter i nätfiske

Nätfiske innehåller ofta misstänkta element och oväntade begäranden som varnar för falsk kommunikation.



Praktiska tips för att
undvika nätfiske på dator

Kontrollera avsändare och länkar

Kontroll av e-postdomän

Verifiera alltid e-postadressens domän för att säkerställa att den är äkta och pålitlig.

Förhandsgranska länkar

Granska alltid länkar innan klick för att undvika att hamna på falska eller skadliga webbplatser.

Ditt Apple-ID är tillfälligt låst!

Från: Apple

Till: Thomas <thomas.carlsson@citedo.se>

Bästa kund,

Vårt system har upptäckt flera misslyckade inloggningsförsök med ditt Apple-ID från okända enheter.

Ditt Apple-ID gör att du kan handla i App Store och iTunes Store.

Kontrollera dina uppgifter här nedanför:

[Logga in nu](#)

Legitim länk till en Google-sida:

<https://w1.google.com/index.html>

Länk till en okänd, eventuellt skadlig sida:

<https://google.com.w1.com/index.html>

- www.google.com (q ersätter g)
- info@ikea.com (l ersätter i)

Microsoft Support <support@micr0soft.com>

Apple Support <noreply@fake-foxmail.com>

Hantera bilagor och nedladdningar säkert

Undvik okända bilagor

Öppna aldrig bilagor från okända eller misstänkta avsändare för att minska risken för skadlig programvara.

Använd antivirusprogram

Använd antivirusprogram för att skanna alla filer innan de öppnas och skydda datorn mot virus.

Legitim länk till en Ikea-sida:

<https://products.ikea.com/a2/>

Länk till en okänd, eventuellt skadlig sida:

<https://ikea.com.products.com/a2>

Legitim länk till en Microsoft-sajt:

<https://office365.microsoft.com/login>

Länk till en okänd, eventuellt skadlig sida:

<https://office365.microsoft.com.login4.com/>



https://
~~http://~~

Användning av säkerhetsprogram och uppdateringar

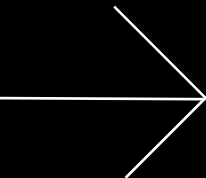
Vikten av uppdateringar

Regelbundna uppdateringar säkerställer skydd mot nya och kända säkerhetshot.

Skydd mot nätfiske

Uppdaterade säkerhetsprogram hjälper till att blockera nätfiskeförsök effektivt.

Praktiska tips för att
undvika nätfiske på
mobiltelefon



Varning för sms och chattmeddelanden med länkar

Viktig information!

Från: Bent Karlsson <mrfly773884@hotmail.com>

Till: Thomas <thomas.carlsson@citedo.se>

Hej.

Vi har hemlig information till dig. Klicka på den här länken:

Viktig information till dig!

Vänliga hälsningar

Company Inc.

Riskfyllda länkar

Länkar i sms och chattar kan vara farliga om avsändaren är okänd eller meddelandet kräver snabb åtgärd.

Verifiera alltid avsändare

Kontrollera alltid vem som har skickat meddelandet innan du klickar på någon länk för att undvika bedrägerier.

Undvik brådska vid klick

Var skeptisk mot meddelanden som skapar brådska och undvik att klicka utan noggrann kontroll.

Kontrollera en länk, men med stor försiktighet

Man skall kunna kolla länkar i tex ett mail genom att hålla på länken länge så skall det komma upp en "förhandsgranskning" av adressen, för att då se om den tex pekar på något helt annat

<https://ikea.com.products.com/a2>

Mobilens säkerhetsinställningar och appar

Appbehörigheter

Hantera appars behörigheter för att skydda personlig information och säkerställa säker användning.

Automatiska uppdateringar

Aktivera automatiska uppdateringar för att säkerställa att mobilen är skyddad mot nya säkerhetshot.

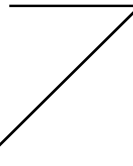
Rapportera och blockera misstänkta meddelanden

Blockera misstänkta avsändare

Mobilen kan blockera sms och samtal från misstänkta avsändare för att skydda användaren från nätfiske.

Rapportera nätfiske

Rapportera misstänkta meddelanden till operatören eller myndigheter för att stoppa nätfiske och skydda andra.



Vad gör man om man
blivit utsatt för nätfiske?

Omedelbara åtgärder vid misstänkt incident

Byt lösenord snabbt

Att omedelbart byta lösenord minskar risken för fortsatt obehörig åtkomst efter en nätfiskeattack.

Avsluta misstänkta sessioner

Stäng alla aktiva sessioner som verkar misstänkta för att förhindra ytterligare intrång.

Isolera infekterade enheter

Koppla bort infekterade enheter från nätverket för att begränsa skadan och spridningen av skadlig kod.

Vikten av att rapportera till rätt instanser

Rapportera till IT-ansvariga

Informera IT-ansvariga snabbt om incidenter för effektiv teknisk hantering och förebyggande av skador.

Kontakta banken

Anmäl incidenter till banken för att skydda finansiella tillgångar och förhindra bedrägerier.

Anmäl till polisen

Vid allvarliga incidenter bör polisen kontaktas för rättslig hjälp och utredning.

Förebyggande utbildning och informationsspridning inom föreningen

Regelbunden utbildning

Föreningen bör hålla regelbundna utbildningar för att öka medvetenheten om nätfiske bland medlemmarna.

Informationsdelning

Delning av aktuell information om nätfiske hjälper till att hålla medlemmarna uppdaterade och vaksamma.

Stärkt säkerhetskultur

Utbildning och informationsdelning bygger en starkare säkerhetskultur och minskar risken för attacker.

Sammanfattning och viktiga nyckelpunkter

Allvarligt hot från nätfiske

Nätfiske utgör ett betydande hot mot idrottsföreningars digitala säkerhet och kräver uppmärksamhet.

Vikten av kunskap och rutiner

Rätt säkerhetsrutiner och ökad kunskap hjälper till att effektivt skydda mot nätfiskeattacker.

Snabb reaktion vid misstanke

Att agera snabbt vid misstänkt nätfiske kan minimera skador och skydda föreningens information.

