Håll dina appar och din programvara uppdaterade

Patchar åtgärdar säkerhetsbrister som kan möjliggöra obehörig åtkomst till kärnkraftskontrollsystem och känsliga data.

Var vaksam. Var cybermedveten.

Aktivera flerfaktorsautentiseri ng (MFA)

MFA lägger till ett avgörande skyddslager för åtkomst till kritiska system, nätverk och operativa verktyg.

Var vaksam. Var cybermedveten.

Se till att ditt hemnätverk är säkert

Att ändra standardlösenordet på din router och se till att den inbyggda programvaran är uppdaterad minskar risken för hackning.

Var vaksam. Var cybermedveten.

Varför använda ett VPN för extra säkerhet?

Ett VPN hjälper till att säkra fjärråtkomst till kärnkraftssystem och konfidentiella dokument, vilket minskar risken för avlyssning.

Var vaksam. Var cybermedveten.

Glöm inte den fysiska säkerheten

Att säkra fysisk åtkomst är lika viktigt som digital – lås alltid terminaler och förvara tryckt material relaterat till verksamheten säkert.

Var vaksam. Var cybermedveten.

Delar du känslig information på sociala medier?

Att publicera platsdata eller projektmedverkan kan avslöja sårbarheter – undvik att dela allt som kan användas för att rikta in sig på personal eller anläggningar.

Var vaksam. Var cybermedveten.

Följ alltid företagets policyer och rutiner

Följ alltid interna protokoll för att skydda nationell infrastruktur och regelefterlevnad.

Var vaksam. Var cybermedveten.

Se upp för social ingenjörskonst

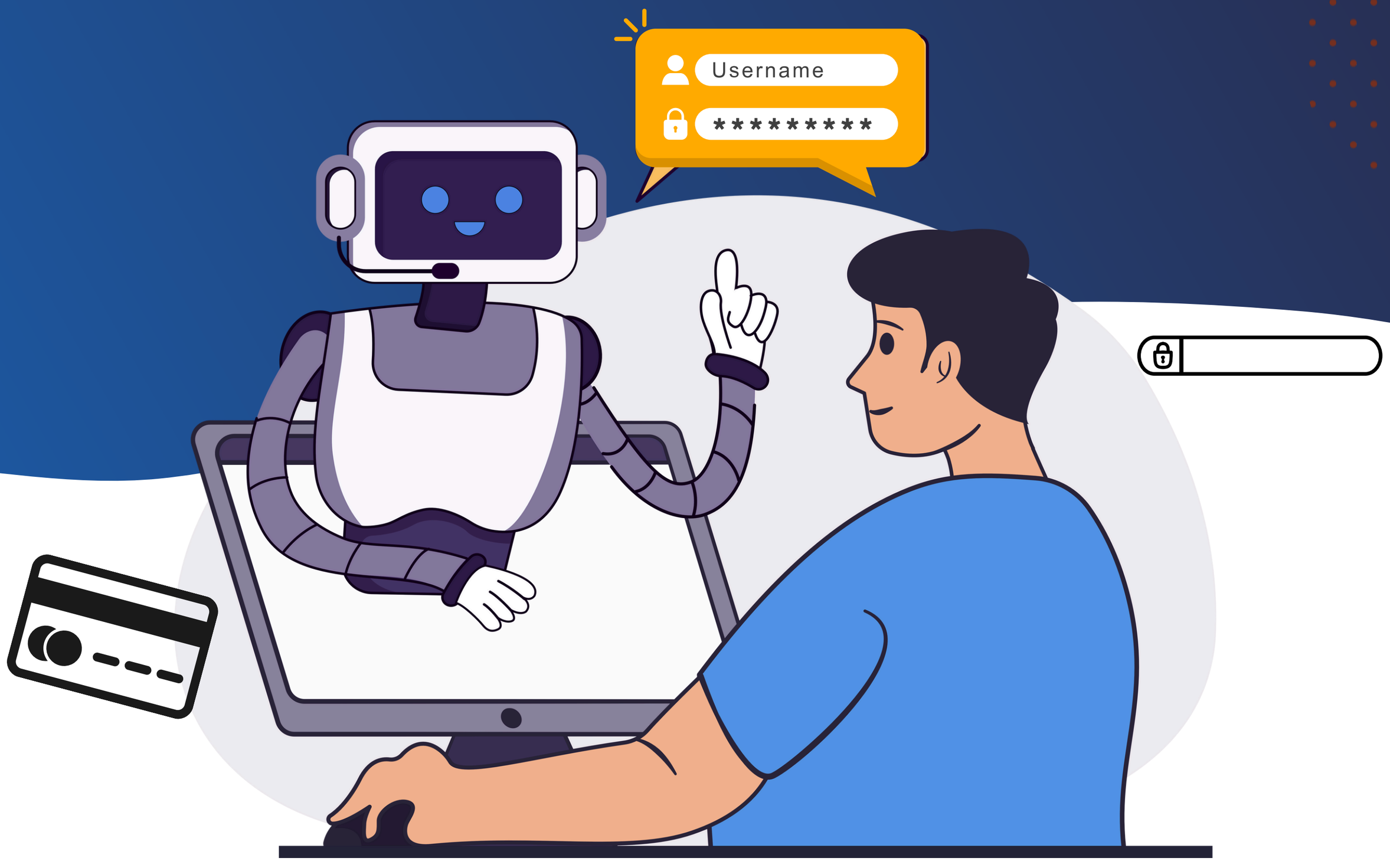
Angripare kan utge sig för att vara inspektörer, leverantörer eller tillsynsmyndigheter – verifiera alltid innan du beviljar åtkomst eller information.

Var vaksam. Var cybermedveten.

Tänk innan du skriver

Bedragare använder falska AI-chattrobotar för att utge sig för att vara supportmedarbetare, kollegor eller betrodda tjänster. De syftar till att lura dig att dela personuppgifter, klicka på skadliga länkar eller göra betalningar.

Pausa innan du svarar – lita inte på alla chatbotar!



Var vaksam. Var cybermedveten.

5 tydliga tecken på en social engineering-attack

Meddelandet kommer oväntat

Oombedda meddelanden – särskilt de som verkar komma från tillsynsmyndigheter, leverantörer eller IT – bör behandlas med försiktighet.

Den begärda åtgärden verkar ovanlig

Var uppmärksam om du blir ombedd att kringgå protokoll, dela driftsdata, installera icke-godkänd programvara eller åsidosätta åtkomstkontroller.

Den begärda åtgärden verkar riskabel

Om det kan påverka kärnsäkerhet, systemtillgänglighet eller efterlevnad av regler att slutföra åtgärden, stoppa och eskalera den.

En ovanlig bilaga eller URL

Skadliga länkar eller filer kan vara förklädda som inspektionsrapporter, säkerhetsuppdateringar eller efterlevnadsdokument – verifiera innan du öppnar.

Det finns en känsla av brådska

Hotaktörer kan hänvisa till avstängningar, revisionsfel eller säkerhetsintrång för att driva på snabba åtgärder – sakta ner och validera.

Var vaksam. Var cybermedveten.

Ta inte illa upp för nätfiskebete!

Nätfiskemejl ser ut som legitima förfrågningar från kända enheter och uppmanar dig ofta att klicka på länkar, ladda ner bilagor eller lämna ut känslig information.

Kom ihåg att tänka innan du klickar

Var vaksam. Var cybermedveten.

Tänk innan du skannar

Quishing-attacker använder QR-koder i nätfiskemejl som ser ut att komma från legitima avsändare. Målet? Att få dig att skanna, klicka på eller dela känsliga uppgifter.

Pausa innan du skannar – ta inte betet!

Var vaksam. Var cybermedveten.

Tips om nätfiskemedvetenhet

Misstänkta länkar i e-postmeddelandet

Var försiktig om webbadressen du ser när du håller muspekaren över sidan inte matchar avsändaren – eller om du dirigeras till en inloggningssida som utger sig för att vara en byrå, leverantör eller intern portal.

Dålig stavning och grammatik

Nätfiskemejl som riktar sig mot kritisk infrastruktur kan fortfarande innehålla fel. Felstavningar i avsändarnamn eller policyreferenser är vanliga varningssignaler.

Begäran om känslig information

Dela aldrig inloggningsuppgifter, åtkomsttokens eller operativa data via e-post. Ring alltid en känd intern kontakt för att verifiera ovanliga förfrågningar.

Underförstådd brådska eller hot

Nätfiskekampanjer riktade mot energisektorn utger sig ofta för att vara brådskande regleringsåtgärder eller säkerhetsvarningar – pausa innan du reagerar.

Misstänkta domäner

Titta noga – angripare kan förfalska domäner som tillhör kärnkraftsmyndigheter, leverantörer eller interna verktyg med hjälp av subtila karaktärsbyten.

Var vaksam. Var cybermedveten.

Använd alltid starka, unika och konfidentiella lösenord

Dina lösenord måste vara unika, privata och lätta för dig att komma ihåg, utan att vara lätta för en angripare att gissa.

Var vaksam. Var cybermedveten.

Tips för lösenordssäkerhet

Återanvänd inte lösenord

Om ett dataintrång läcker ett av dina konton kan angriparen få åtkomst till andra konton med hjälp av dina återanvända lösenord.

Lämna inte lösenord framme i synhåll

Lämna inte lösenord på en osäker plats, till exempel på en post-it-lapp, i en dagbok eller i en okrypterad textfil.

Dela inte dina lösenord

Dela aldrig dina lösenord eller konton med någon, inte ens dina kollegor.

Skapa långa och enkla lösenord

Använd en serie orelaterade ord för att skapa långa, enkla lösenord snarare än korta och komplexa.

Använd metoder för flerfaktorsautentisering

Använd den säkraste metoden för flerfaktorsautentisering som finns tillgänglig för dig, till exempel en autentiseringsapp.

Var vaksam. Var cybermedveten.