

## Prevenációs lehetőségek:

- Az intézmény/vállalkozás érzékeny (tehát védendő) információinak meghatározása.
- Az intézmény védendő/bizalmas információit ismerők körének meghatározása.
- Egyértelmű, profiltiszta feladat-meghatározások, munkaköri leírások és hozzáférési jogosultságok.
- Biztonsági előírások, belső szabályzók felállítása (a nemzetközi, illetve a magyar partnerekkel folytatott kommunikációra vonatkozóan, stb.), betartása és betartatása, időszakos ellenőrzése.
- A munkatársak folyamatos jellegű, biztonsági szempontú felkészítése.
- Külsős látogatók regisztrálása, kísérése és folyamatos figyelemmel követése.
- A kompromittáló szituációk kerülése; az intézmény iránti lojális magatartás munkaidőben és azon túl is.
- Gyanús eseményeket követően kapcsolatfelvétel az Alkotmányvédelmi Hivatallal.

A bizsagságtudatossági szabályozások kidolgozásában munkatársaink szívesen nyújtanak segítséget.

***Forduljon kollégáinkhoz, kérjen időpontot tanácsadásunkra!***

***A bizsagság megteremtése csapatmunka!***

***Elérhetőségünk:  
awareness@mail.ah.gov.hu***

## ALKOTMÁNYVÉDELMI HIVATAL

### AWARENESS PROGRAM



## ADMINISZTRÁCIÓS MUNKAKÖRÖK BIZTONSÁGI KIHÍVÁSAI

**Az Alkotmányvédelmi Hivatal  
Awareness programjának  
tájékoztatóját tartja a kezében.**

Célunk, hogy olyan kockázati tényezőkről, lehetséges veszélyforrásokról adjunk tájékoztatást, amelyek a biztonsági tudatosság hiányában jelentkezhetnek, valamint az említett veszélyek kivédésére alkalmas tippekkel, gyakorlati tanácsokkal lássuk el Önt.

Minden intézmény, cég, vállalkozás alkalmaz adminisztrációs feladatokat ellátó munkatársakat, akik az elmúlt évtizedek hagyományos titkárnői feladatain túl, mint a gyors- és gépírás, szövegszerkesztés, a 21. századra jellemző szervezési-menedzselési tevékenységet is ellátnak. A vezetők irányítási funkciója jó és pontos adminisztrációt, szervezést, egyeztetést követel, amely csak megfelelően összehangolt munkafolyamatban lehet sikeres, ennek kialakításában és működtetésében pedig komoly szerep hárul a titkárnőkre, asszisztensekre. Számos olyan, értéket hordozó információnak vannak birtokában ezen kollégák, amelyek illetéktelen kezekbe való kerülése negatív hatással lehet az intézményre, a dolgozókra, a munkatevékenységre.

**Esettanulmányok:**

- Egy vállalat titkárnőjét magánéleti körülményei kapcsán igyekezett presszionálni egy személy, aki így kívánt jogosulatlan előnyhöz jutni.
- Egy külföldi delegáció tagjai számítástechnikai kérdésben kértek segítséget a titkárságon, hogy így kémprogramokat, adathalász vírusokat juttassanak az intézmény belső hálózatába.
- Ajándékok, virágcsokor, bonbon átadásával igyekezett egy személy szimpátiát ébreszteni a titkárság dolgozóiban, hogy a későbbiekben saját érdekei mentén felhasználhassa az így kialakult nexust.
- Vezetőkhöz tolokodóan bejutni kívánó személy több titkárnőnél is bejelentkezett, majd felváltva hivatkozott rájuk, már-már követhetlenné téve a cselekményt.

**A felelőtlen kommunikáció lehetséges  
következményei:**

- adatlopások, visszaélések,
- gazdasági/ipari hírszerzés,
- pszichológiai manipuláció, befolyásolás,
- a hírnév romlása, piaci pozícióvesztés.

***Keressen minket, ha az alábbiak  
valamelyikét tapasztalja:***

- munkahelyének informatikai rendszerét támadás érte,
- gyanús, feltehetően a pozíciójának szólo kapcsolatépítést tapasztal,
- kompromittáló szituációba keveredett, amely a későbbiekben felhasználható Ön ellen,
- munkáltatójának bizalmas információi idegen kezekbe kerültek.