SÜEM 2. Dönem

# BİLİŞİM TEKNOLOJİLERİ

Prof. Dr. Zayde Ayvaz

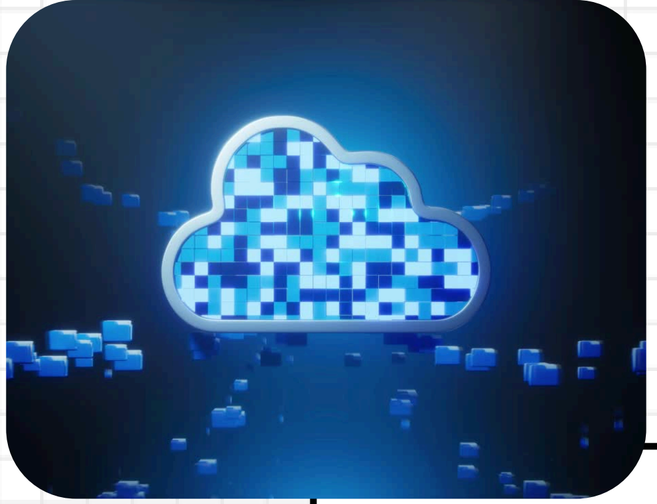
# Dijital Güvenlik ve Mahremiyet (Siber Hijyen)

# Neden Önemli

Neden güvenlik? (hesap ele geçirme, veri kaybı, dolandırıcılık)

Bugün: parola + 2FA + phishing + cihaz güvenliği + gizlilik

Çıktı: herkes “mini güvenlik kontrolü” yapacak



# Gerçek Hayat Senaryoları

1. “Şifrem sızdı” → hesaplar tek tek ele geçirilebilir
2. “Arkadaşımın hesabından link geldi” → sosyal mühendislik olabilir
3. “Cloud linki herkese açıkmış” → kişisel dosyalar görünmüş olabilir
4. “Telefon kayboldu” → yedek ve ekran kilidi yoksa veri riski

***En son ne zaman şifre değiştirdin / 2FA açtın?***

# Tehdit Haritası

1) Kimlik avı (Phishing): e-posta/SMS/DM ile kandırma
2) Zayıf parola: tahmin edilebilir veya tekrar kullanılan parola
3) Cihaz riski: güncelleme yok, ekran kilidi zayıf
4) Paylaşım hatası: “herkese açık link”, yanlış izin
5) Zararlı yazılım: şüpheli dosya/uygulama, crack programlar

# Parola Güvenliği: Altın Kurallar

- Aynı parolayı birden fazla yerde kullanma
- Parola uzun olsun: 12–16+ karakter iyi pratik
- “Kelime+kelime+kelime” (passphrase) yaklaşımı daha güvenli ve hatırlanır
- Tahmin edilebilir şeylerden kaçın: ad, doğum tarihi, 123456
- Parolayı paylaşma / not defterine yazıp bırakma

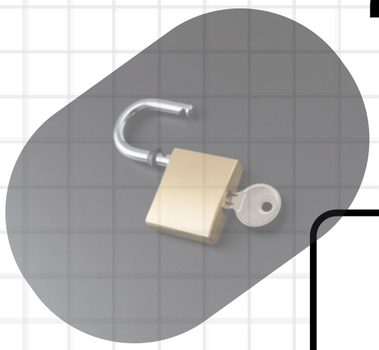
*Örnek (iyi): Deniz!Kitap-Kahve_2026*

*Örnek (kötü): ahmet123, password, 123456*

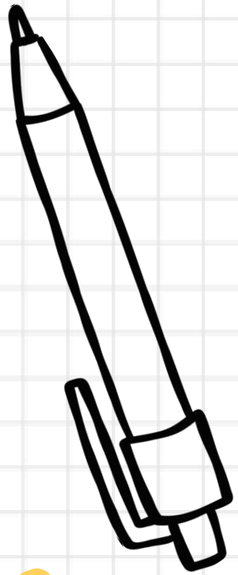
# Parola Yöneticisi (Niye Kullanılır?)

- Her hesap için benzersiz güçlü parola üretir
- Otomatik doldurma ile pratiklik sağlar
- Tek bir ana parola + biyometrik ile yönetim kolaylaşır
- iPhone/Mac: iCloud Keychain; Windows: Edge/Chrome şifre yöneticileri

# 2FA/MFA: Hesabı Gerçekten Korumak



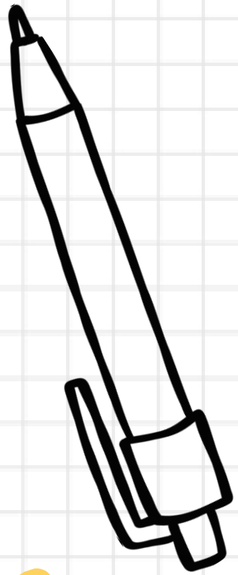
- Şifre çalınsa bile ikinci adım olmadan giriş zorlaşır
- Yöntemler:
- Uygulama kodu (Authenticator)
- SMS kodu (daha zayıf ama hiç yoktan iyi)
- Güvenlik anahtarı (ileri seviye)

*En kritik hesaplar: e-posta, bulut, banka, sosyal medya → 2FA aç.*

# Phishing'i 30 Saniyede Yakalama Kontrol Listesi

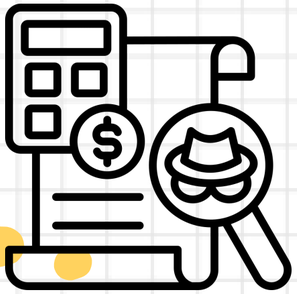
- Gönderen adresi tam kontrol et (benzer yazım tuzakları)
- Mesaj "acil/tehdit/ödül" dili kullanıyor mu?
- Linkin üstüne gel: gerçek adres ne? (kısaltılmış link şüpheli)
- Dosya eki bekliyor muydun? (.exe, .zip, makrolu dosyalar riskli)
- "Şifreni gir" diyorsa → asla linkten giriş yapmaKendin tarayıcıdan siteyi aç, oradan giriş yap



*En kritik hesaplar: e-posta, bulut, banka, sosyal medya → 2FA aç.*

# Sosyal Mühendislik: İnsan Zayıf Halkadır


- Dolandırıcılık sadece teknik değil, “ikna” işidir
- Örnekler:
- “Hocam ben öğrencinizim, acil dosya lazım”
- “Kargonuz var, linke tıklayın”
- “Hesabınız kapanacak”
- Savunma: yavaşla, doğrula, resmi kanaldan kontrol et



# Cihaz Güvenliği (Telefon + Bilgisayar)

- Ekran kilidi: güçlü PIN / FaceID/TouchID
- Güncellemeler: işletim sistemi + tarayıcı + uygulamalar
- Uygulama izinleri: gereksiz erişimleri kapat (konum, mikrofon vb.)
- Ortak bilgisayarda: çıkış yap, otomatik doldurmayı kapat
- Halka açık Wi-Fi: hassas girişlerde dikkat (mümkünse VPN/kişisel hotspot)


# Bulut Paylaşımı ve Mahremiyet (Drive/OneDrive/iCloud)

- Link paylaşımı ayarı:
- “Herkese açık” (riskli)
- “Bağlantıya sahip olan” (kontrollü)
- “Belirli kişiler” (en güvenli)
- İzin seviyesi: görüntüle / yorum / düzenle
- Paylaştığın klasörleri düzenli gözden geçir: “Kimlerde erişim var?”
- Ödev/rapor paylaşırken: çoğunlukla yorum yeterlidir