Batman Üniversitesi

Son Kullanıcı Siber Güvenlik Rehberi

Siber saldırılar bilgi ve teknoloji çağının en önemli mevzusu durumundadır. Bu konuda siz de mağduriyetler yaşamak istemiyorsanız ve kurumunuzun siber güvenliğine katkıda bulunmak istiyorsanız yönergeyi takip edebilir, maddi ve manevi zararların önüne geçebilirsiniz.

Bilgi Güvenliği Nedir?

Kişiye ait şahsi bilgilerin (mailler, yazışmalar, dokümanlar..) ve kuruma ait özel verilerin çalınma, ele geçirilme, aleyhte kullanma, zarara uğratma gibi zaafiyetlere mahal bırakmayacak şekilde gizlilik, bütünlük ve erişilebilirliğinin korunması için alınan tedbirler, yapılan iş ve işlemlerin tümüdür.

Neden Bilgi Güvenliği?

- Şahsi bilgileriniz çalınabilir, aleyhinizde kullanılabilir.
- Emek verdiğiniz projeleriniz, çalışmalarınız kötü niyetli kimselerin eline geçebilir.
- Spamlerle eposta hesaplarınız ele geçirilebilir, sizin adınıza başkalarına mailler yollanabilir.
- İnteraktif bankacılık hesaplarınız ele geçirilebilir, banka hesabınız boşaltılabilir, adınıza krediler çekilebilir.

- Şahsi bilgisayarınıza sızan kötü niyetli kimseler bilgisayarınızı kaynak olarak kullanıp siber suçlar işleyebilir ve neticede ciddi suçlamalarla karşılaşabilirsiniz.
- Sosyal hesaplarınız (facebook, Twitter, Pinterest, Instagram..) ele geçirilebilir.
- Sizi zor durumda bırakacak paylaşımlarda bulunulabilir.
- Mobil uygulamalarla telefonunuz ele geçirilebilir, dinlenebilir, izlenebilir, yüksek maliyetli faturalarla karşılaşabilirsiniz.

- Kişisel bilgilerinizin ele geçirilmesi ile; Özel hayatınız izlenebilir, sosyal hayatınız sabote edilebilir, toplum içindeki konumunuz zedelenebilir.
- Kişisel bilgisayarınıza istem dışı kurduğunuz yazılımlarla kötü niyetli kişilerin ortam dinlemesine takılabilir, digital kayıt altına alınabilirsiniz.
- Vatandaşlık ve sosyal güvenlik numaranız, şahsi kimlik bilgilerinizin ele geçirilmesi ile çeşitli dolandırıcılık suçlamalarıyla karşılaşabilirsiniz.
- Bilgilerinizin ele geçirilmesi ile adınıza sahte kimlikler, pasaportlar hazırlanabilir.
- Bilgisayarınız ve akıllı telefonlarınız gerekli güvenlik tedbirleri alınmadığı takdirde hacklenebilir ve tüm dokümanlarınız kullanılamaz hale getirilebilir, değiştirilebilir, yayınlanabilir.

Ne Yapmalıyım?

Siber güvenlik yazılımsal ve donanımsal tedbirlere ek olarak bilinçli kullanıcı toplumu yaratmak ile sağlanabilir. Yapmanız gereken en önemli şey önlem almak için zaman ayırmak ve dikkatli davranmaktır. Telefon, tablet, pc, yazıcı ve diğer bilişim ürünlerinizin fiziksel güvenliğini sağladığınızda ciddi bir yol katetmiş olursunuz. Kalan detaylar ise siber güvenlik konusundaki bilinç düzeyinize bağlı olarak değişmektedir.

- Bilgi güvenliğinin en önemli parçasını kullanıcıların duyarlılıkları oluşturmaktadır.
- Oluşan güvenlik açıkları son kullanıcıların zaafiyetlerinden kaynaklanmaktadır.
- Saldırganlar son kullanıcıların açıklıklarını kullanıp ağa, sisteme sızdıklarından son kullanıcılar bireysel siber güvenliklerine önem vermelidirler.
- Bir kullanıcının güvenlik açıkları tüm sistemi etkileyebilmektedir.
- Siber güvenlik tehditlerini ciddiye alınız. Tedbirlerinizi almak konusunda rehavete kapılmayınız. Bir şey olmaz demeyiniz!
- Cihazlarınızın fiziksel güvenliğini sağlayınız.
- Masaüstü bilgisayarınızı, telefonunuzu, laptopunuzu kullanmadığınız durumlarda müdahaleye kapalı olması için kilidini aktifleştiriniz.
- Bilgisayarınız ile işiniz bittiğinde kapalı durumda tutunuz.
- Sitelere üye olmak ve program indirmek, oyun oynamak için mail ile kayıt istenen, aktivasyon gerektiren sitelere asla ama asla resmi kurumsal mail adresiniz ile giriş yapmayınız. Mail adresinizi portallarda paylaşmayınız. Spam mail listelerine alındığınızda rahatsız edilmekten kurtulamazsınız.
- Büyük - küçük harf, rakam ve özel karakter (?*+()/!.) kullarak karışık parolalar oluşturunuz. Örn: Passw0rd2017!

- Şifrelerinize; klasik parolalar (123456789, fener06, superman, 345543,123321, batman, 1q2w3e, parola34, 123qwe,qwe123, doğum tarihinizin gün ay yılını (010789) il plaka numaralarını (7234, 2172, 2121,4772..) ve masanızda bulunan çiçek, obje, çizgi film kahramanlarının isimlerini vermeyiniz.
- Şifrenizin zorluk seviyesini buradan öğrenebilirsiniz: http://www.bilgimikoruyorum.org.tr/?b223_yaparak_ogrenelim
- İnsanların zaaflarını ve güvenlerini kullanarak isteğiniz bilgiyi ve veriyi ele geçirme sürecine Sosyal Mühendislik denir. İnsanlar çoğu zaman kandırılma olasılıklarının düşük olduğunu düşünür ve genellikle güvenliklerini arka plana iterler. Sosyal mühendislikteki insan faktörü en büyük tehdit olarak karşımıza çıkabilmektedir. Çünkü, sosyal mühendislikte duyduğumuz güven en büyük zaafımız olabilmektedir.
- Sosyal Mühendislikte, veri hırsızı kurbanını analiz ederek kendisinin merakından, inancından, güven, para, cinsellik düşkünlüğünden ve makam, mevki, ego gibi hırslarından istifade ederek zayıf yanlarından istifade eder. Tedbirli olunuz.
- Telefon aracılığıyla yapılan sosyal mühendislik yöntemlerine karşı dikkatli olunmalıdır. Size gelen aramalarda tanımadığınız biri kendisini herhangi bir birimin personeli olarak tanıtıp bilgi ve belge talebinde bulunduğunda, bu gibi durumlarda arayan kişinin bilgilerini teyit etmeden herhangi bir bilgi paylaşmamanız önemlidir.
- Sosyal mühendislik yöntemlerine karşı tedbirli olunuz. Şifreleriniz aynı olmasın, ortalık yerde kimseye söylemeyiniz, şifrenizi girerken mırıldanmayınız, kimse görmeyecek şekilde şifre, pin, parolanızı giriniz.
- Üçüncü kişilerin kullanımına açtığınız PC, laptop ve telefonlarınızı ayrıca oturum ekranları açarak kullanımlara açınız.
- Dosyalarınızı bulut servislerinde (Google Drive, Microsoft Onedrive, Azure, Dropbox..) depolayınız. Cryptolocker gibi bilgisayarınıza bulaştığında dosyalarınızın tümünü şifreleyip kullanılamaz hale getiren virüslere karşı yedeğiniz olmuş olur.
- Kişisel ve kurumsal mail hesaplarınızı başka hesaplarınıza entegre etmek suretiyle yedekleyiniz. Gmail ve Hotmail gibi servislerde kolayca entegrasyon gerçekleştirebilirsiniz.
- Gmail,Dropbox gibi hesaplarınızda çift basamaklı doğrulamayı açmanız durumunda; şifrenizi ele geçirmeleri durumunda bile hesabınız üçüncü şahısların erişimlerine kapalı olacaktır.

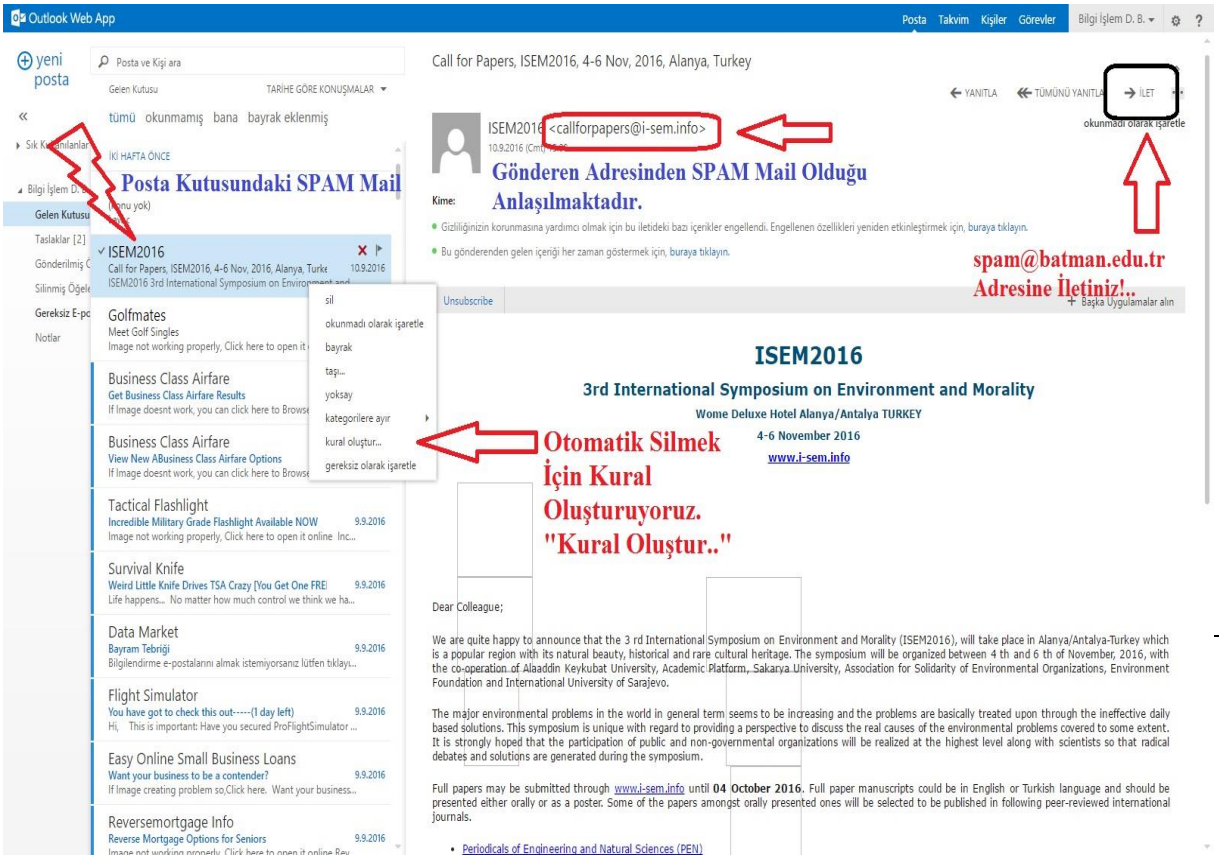
- Outlook gibi yazılımlar kullanmanız her ne kadar hızlı erişim sağlamak açısından önemli olsada bilgisayarınızın ele geçirilmesi durumunda Outlook üzerinde açık olan hesaplarınızın tamamının ele geçirilmiş olacağını unutmayınız, tedbirli davranınız.
- Ebys, mail, wireless şifrelerinizi bir yerlere yazmayınız, kimse ile paylaşmayınız.
- Ebys, mail ve wireless oturumlarınızı en son açmış olduğunuz bilgisayar veya telefondan kapatmadan çıkmayınız. Hesaplarınızı açık bırakmamaya özen gösteriniz.
- Ebys, mail ve wireless oturumlarınızı açtığınızda şahsi bilgisayarınız değilse "Şifreyi Hatırla" seçeneğini aktifleştirmeyiniz.
- Elektronik imzanız varsa şahsi bilgisayarlarınız dışında başka makinelere bağlanarak işlem yapmaktan kaçınınız. Kimseye vermeyiniz. E-imza şifrenizi ilk günkü haliyle kullanmayınız mutlaka değiştiriniz. Ebys sistemindeki işlemlerin onayında kullanılan elektronik imzalar, ıslak imza ile aynı yasal yükümlülükler taşımaktadır.
- Tüm şifrelerinizi periyodik olarak değiştirmekten çekinmeyiniz.
- Bilgisayarlarınıza kaynağı belli olmayan yazılımlar kurmayınız, yazılımlar indirmeyiniz. Lisanslı ürün kullanmaya özen gösteriniz. İndirdiğiniz korsan film, müzik ve dosyalar genellikle virüslüdürler. Unutmayınız: Bu program ve dosyalar belli amaçlar için indirilmeye, kullanıma açılıp paylaşılmaktadır.
- Kırılmış (Crack) program siteleri, oyun siteleri, sohbet siteleri gibi riskli web sitelerine girmekten kaçınınız.
- İnternet sayfalarında surf yaparken anlık çıkan popup şeklindeki onay kutularına "evet", "tamam", "kabul ediyorum" şeklindeki seçenekleri tıklamayınız.
- Dosyalarınızı harici HDD, CD, DVD USB gibi donanımlarla taşımaktan kaçınınız. Dosyalarınızı taşımak konusunda bu donanımların kullanımını zorunlu hissediyorsanız kullandıktan sonra ilk fırsatta bu donanımlardan kaldırıp siliniz.
- Harici donanımları güvenmediğiniz bilgisayarlarda açmayınız, güncellemeyiniz. Virüs taramasından geçirmeden açmayınız.
- Kaynağını bilmediğiniz ve korsan yazılım taşıma riski bulunan harici USB, HDD, CD gibi donanımları bilgisayarınızda çalıştırmayınız.
- Kampüs ağına bağlı olan bilgisayarlarınız günlük olarak virüs taramasından geçirilmektedir. Ancak, bilgisayarınızda gün içinde anormal bir durum, sayfaların açılmasında bir yavaşlama, donma gibi durumlar olduğunu hissettiğiniz zaman manual olarak virüs taramasından anlık olarak geçirmeniz korunmanıza yardımcı olacaktır.
- Virüs taramasının yetersiz kalması durumunda verilerinizi yedeklemek suretiyle bilgisayarınıza format atmanız sizi zararlı yazılımların etkilerinden koruyacaktır.

- Bilgisayarınızı, tablet ve telefonunuzu periyodik olarak güncelleştiriniz. Bu şekilde varsa zero-day (anlık) güvenlik zaafiyetlerini gidermiş olursunuz .
- Bilgisayarınızdaki anti virüs yazılımları sizi virüslerden, trojan, keylogger, worm gibi bilgisayarınıza yerleştiklerinde bilgisayarınıza zarar veren, bilgilerinizi bilginiz dışında üçüncü şahıslarla paylaşan, iş ve işlemlerinizi izleyip raporlayan ve bu raporları dışarıya periyodik olarak gönderen zararlı program ve yazılımlardan korurlar. Bu yüzden bilgisayarınızın güncellenmesi ve periyodik olarak taramadan geçirilmesi önemlidir.
- Klavye ile bilgisayar arasına bağlanan ve dışarıdan bakıldığında dönüştürücüden farkı olmayan cihazlar donanımsal keyloggerlardır. Bu donanımlar klavyenize bastığınız tüm tuşları kaydedip depolarlar. Yerleştirilen donanımlar veya ortama yerleştirilen gizli kameralar ile hareketleriniz ve konuşmalarınız kaydedilebilir, tuşlamalarınız izlenebilir ve şifreleriniz ele geçirilebilir.
- Bu tür donanımsal cihazlara karşı önlem olarak her gün klavyeniz ile bilgisayar bağlantınızı kontrol edip, herhangi bir cihaz takılıp takılmadığını kontrol etmeniz gerekmektedir.
- Bir ağ grubu içerisinde paylaşıma açılmış dosyaları virüs taramasından geçirmeden indirmeyiniz. Bu gibi yerlerde önemli dosyalarınızı paylaşmayınız.
- Unutmayınız: bu gibi platformlardan paylaştığınız dosyalar bir şekilde üçüncü şahıslar tarafından görülebilir, işlenebilir, silinebilir ve başka yerlerde yeniden paylaşıma açılabilir.
- Dosya paylaşım yerlerinde oldukça fazla virüslü dosya, program ve doküman bulunabilmektedir. Bu gibi yerlere itibar edilmemesi önem taşımaktadır.
- Paylaşıma açtığınız dosyalarınızı gelişmiş seçeneklerden gizli paylaşıma ve sadece belirli kişilerin erişimine açmanız verilerinizin güvenliği açısından önemlidir.
- Paylaşımlarınız hedef kişiye ulaştıktan sonra dosya paylaşımına kapatmanız önemlidir.
- Mobil telefonlarınıza indirdiğiniz uygulamalar konusunda dikkatli olmalısınız. Kaynağı belli olmayan uygulamaların çoğu ortam dinlemesi, veri aktarımı ve kaynak tüketimi için tasarlanmıştır.

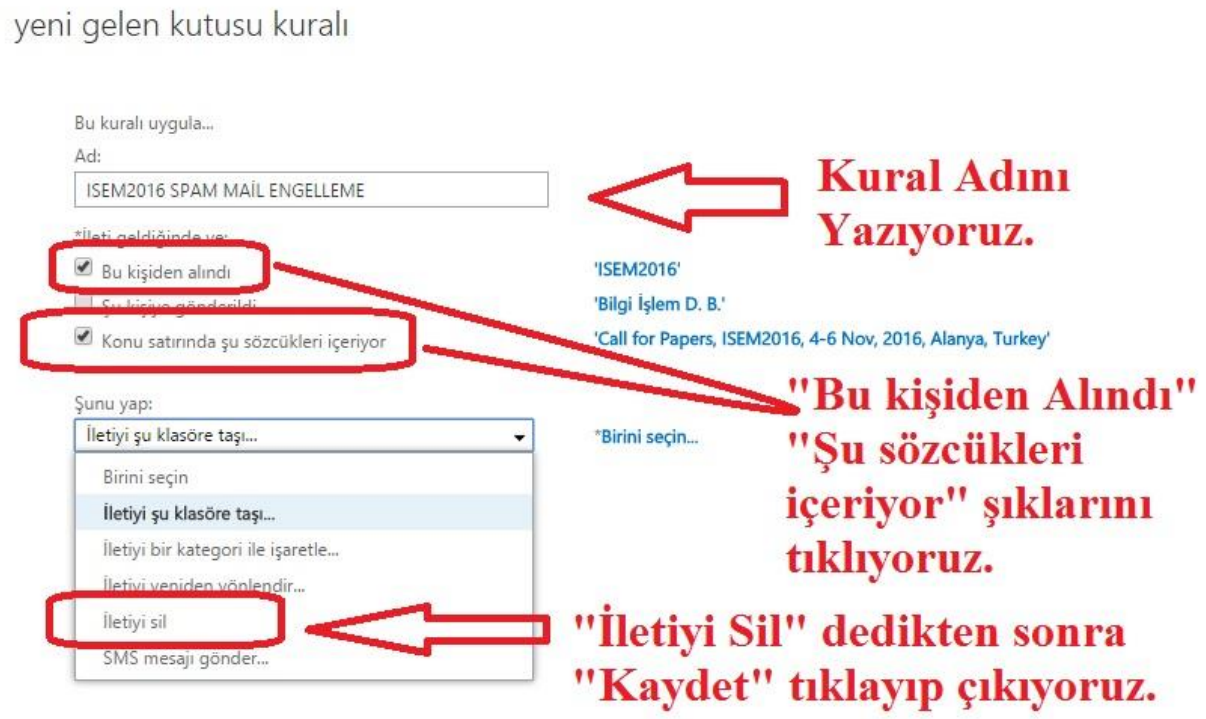
Spam Maillere Nasıl Müdahale Etmeliyim?

- Spam maillerle mücadele önemlidir: Hem maddi manevi zararlara yol açabilirler hem de sistem kaynaklarının tükenmesine, yavaşlamasına yol açarlar.
- Spam mailin güvenlik duvarı ve anti spam modülünü aşması durumunda size rahatsızlık vermemesi için yapılması gerekenler verildiği üzeredir.
- Spam mailler ile ilgili yapılacaklar:
  - ✓ Tanımadığınız, bilmediğiniz kişilerden geldiğini düşündüğünüz maillerin spam olma olasılıkları yüksektir.
  - ✓ E-posta ile gelen eklentiyi açmadan evvel kaynağını kontrol ediniz. Maili virüs taramasından geçiriniz.
  - ✓ Gönderici kısmındaki mail adresinin kurumsal kimliğini kontrol ediniz, genellikle spam maillerin gönderici adresleri göze batan ilginç isimler olur.
  - ✓ Mailin konusunu ve içeriğini inceleyiniz, sizi ilgilendirmediğini düşünüyorsanız spam maildir.
  - ✓ Spam mailleri spam@batman.edu.tr adresine iletiniz.
  - ✓ İlettikten sonra sağ tıklayıp "Yoksay" yada "Gereksiz Olarak İşaretle" seçeneklerini tıklayıp sizi rahatsız etmelerini önleyiniz.
  - ✓ E-posta içindeki linklerin üzerine gelerek hedef internet sayfasını ve güvenilirliğini kontrol ediniz.
  - ✓ Spam olma riski taşıyan mailleri açmayınız.
  - ✓ Eklentilerini indirmeyiniz.
  - ✓ İçeriklerindeki linkleri tıklamayınız.
  - ✓ Başka kullanıcılara yönlendirmeyiniz.
  - ✓ Spam maillere cevap yazmayınız.
  - ✓ Spam mailler toplu olarak gönderildiğinden şahsi algılamayınız. İhbar etmekten çekinmeyiniz.
  - ✓ Gelen maillerden spam olarak algılandığından size ulaşamadığını düşündüğünüz olursa durumu siber@batman.edu.tr adresine iletiniz.
- Spam mailler bazen çok profesyonelce hazırlanabilmekte ve güvenlik duvarı, anti virüs, anti spam gibi güvenlik aşamalarını atlatabilmekte ve son kullanıcılara ulaşabilmektedir. Bu tür saldırılara bireysel olarak yoğun bir şekilde maruz kaldığınızda Siber Güvenlik Birimi ile irtibata geçiniz.

- ✓ Gönderen adresi ve içeriği kontrol ederek tespit ettiğiniz spam maili sağ üst köşede bulunan "İLET" ile spam@batman.edu.tr adresine göndermeniz durumunda mailin başkalarına da erişmesini engellemiş olursunuz.
- ✓ Gelen maili sağ tıklayıp gelen menüden "Kural Oluştur.." sekmesine gidiyoruz.



- ✓ "Kural oluştur" tıklandıktan sonra açılacak "Yeni Gelen Kutusu Kuralı" penceresinde bizden spam ile ilgili kural yazmamız istenmektedir.
- ✓ Bu pencerede kural adını yazıp, gönderen ve konu satırında geçen kelimelere ilgili maili çağrıştırıyorsa engelleme yapmak için tıklıyoruz. Bu mail tespit edildiğinde ise gelen maili otomatik olarak silmesi için "İletiyi sil" seçeneğini "Şunu yap" menüsünden seçip "Kaydet" deyip çıkıyoruz.



- ✓ Kural oluşturulduktan sonra tekrar spam mailin üstüne sağ tıklayıp "Yoksay" ya da "Gereksiz olarak İşaretle" seçeneklerinden birini seçip bir daha rahatsızlık vermesini engelleyip işlemi bitiriyoruz.

- Herhangi bir siber saldırı olayı ile karşılaştığınızda Siber Güvenlik Birimi ile irtibata geçmeniz önem arz etmektedir.
- Uygulamalı bilgi için *Bilgimi Koruyorum* sitesini takip edebilirsiniz: Tıklayınız.
- Kurumsal Siber Güvenlik Rehberinden de istifade edebilirsiniz: Tıklayınız
- Siber güvenlik konusunda görüş ve taleplerinizi siber@batman.edu.tr adresine iletiniz.

Hafzullah İŞ