



T.C.
Honaz Kaymakamlığı
İlçe Milli Eğitim Müdürlüğü
Kızıyer Hüseyin Avni Özden Ortaokulu

GÜVENLİ İNTERNET VELİ BİLGİLENDİRME FORMU

Doküman No	FRM-38
Sayfa No	1 / 2
Revizyon No	0.0
Revizyon Tarihi	--
Yayın Tarihi	19/12/2024
Kurum Kodu	739611

GÜVENLİ İNTERNET VELİ BİLGİLENDİRME FORMU

10 Maddede Güvenli İnternet Kullanımı

Hayatın neredeyse her alanında evimizde, cebimizde, kafelerde, restoranlarda, AVM'lerde ve aklınıza gelebilecek her türlü ortamda interneti özgürce kullanabiliyoruz. Bu denli büyüyen ve gün geçtikçe gelişmeyi sürdüren internetin, gerek sosyal gerekse iş hayatındaki olumlu katkıları yadsınamaz ancak kimi zaman da pek çok olumsuz durumla da bizi yüz yüze bırakabiliyor. İşte bu noktada olumsuz durumları yaşamamak ya da en azından minimuma indirmek adına birtakım önlemler almak gerekiyor. Peki, güvenli internet kullanımı için yapılması gerekenler neler?

1. Kişisel Bilgileri Profesyonel ve Sınırlı Tutun

Potansiyel işveren veya müşterilerin kişisel ilişki durumunuzu veya ev adresinizi bilmesine gerek yok. Şahsi bilgilerinizi tanımadığınız milyonlarca yabancı kişiye kendi ellerinizle teslim etmeyin.

2. Gizlilik Ayarlarınızı Açık Tutun

Pazarlamacılar sizin hakkınızda her şeyi bilmek isterler aynı zamanda hackerlar da ister tabii. Her ikisi de internet taramalarınızdan ve sosyal medya kullanımınızdan bir çok şey öğrenebilir. Bunun önlemini alabilmeniz için hem web tarayıcıların hem de mobil işletim sistemlerin gizliliğinizi çevrim içi korumak için çeşitli ayarlar bulunmaktadır. Ayrıca Facebook, Instagram ve Twitter gibi büyük sosyal medya uygulamalarının da gizlilik artırıcı ayarları mevcut. Burada sizin yapmanız gereken tüm bu güvenlik ayarlarını detaylı bir şekilde gözden geçirip önemli olanlar başta olmak üzere tüm güvenlik ayarlarınızın açık olduğundan emin olmalısınız.

3. Gördüğünüz Her Linke Tıklamayın

Tehlikeli web sitelerinde de dolaşmamalısınız. Siber suçlular, bu tarz tehlikeli gibi gözükmeyen ancak içerisinde birçok tuzak barındıran sahte içerikleri birer yem olarak kullanırlar. Siber suçlular birçok insanın arama yaptıkları esnada buldukları kaynaklar şüpheli dahi olsa merak duygularına yenik düşeceklerini ve içeriklerin cazibelerine kapılıp gardlarını indireceklerini biliyorlar. Bu tarz dikkatsiz tıklamalar sonucunda kişisel verilerinizin açığa çıkabileceği gibi elektronik cihazlarınıza malware diye tabir edilen kötü amaçlı yazılımların yüklenmesine de sebebiyet verebilir.

4. İnternet Bağlantınızın Güvenli Olduğundan Emin Olun

Halka açık bir yerde, örneğin herkese açık bir Wi-Fi bağlantısı kullanarak çevrim içi olduğunuzda, artık cihazınızın güvenliğinin üzerinde doğrudan kontrolünüz olmadığını bilmelisiniz. Onların tavsiyesine göre eğer banka hesap numaranız gibi önemli bilgileri girecekseniz önce cihazınızın bağlandığı ağın güvenli olduğundan emin olmalısınız. Eğer güvenlik ile ilgili herhangi bir şüpheniz varsa, güvenli bir Wi-Fi ağına bağlanana kadar beklemelisiniz.

Hazırlayan	Onaylayan
Kalite Yönetim Ekibi/ Müdür Yardımcısı Derya KARAHAN	Kalite Yönetim Temsilcisi / Müdür Ramazan ÖZYURT



T.C.
Honaz Kaymakamlığı
İlçe Milli Eğitim Müdürlüğü
Kızılyer Hüseyin Avni Özden Ortaokulu

GÜVENLİ İNTERNET VELİ BİLGİLENDİRME FORMU

Doküman No	FRM-38
Sayfa No	2 / 2
Revizyon No	0.0
Revizyon Tarihi	--
Yayın Tarihi	19/12/2024
Kurum Kodu	739611

5. Ne İndirdiğinize Dikkat Edin

Siber suçluların en önemli amacı, kişisel bilgilerinizi çalmaya çalışan veya bilgisayarınızı kendi kötü çıkarları için kullanmaya çalışan kötü amaçlı yazılımları indirmenizi sağlamaktır. Dolayısıyla şüpheli gördüğünüz veya güvenmediğiniz sitelere ait uygulamaları indirmemelisiniz.

6. Güçlü Şifreleri Seçin

Şifreler, tüm internet güvenliği yapısında en büyük zayıf noktalardan biridir. İnsanlar hatırlanması kolay olan şifreleri seçme eğiliminde olduklarından dolayı şifrelerini basit seçmektedirler. Güçlü bir parola belirleyebilmek için, benzersiz kelime grupları oluşturmalı ve en az 8 karakter uzunluğunda, harfleri, sayıları ve özel karakterleri barındıran şifreler kullanmalısınız.

7. Güvenli Sitelerden Satın Alım Yapın

Çevrim içi bir ürün satın aldığınızda, kredi kartı veya banka hesabı bilgilerinizi kullanmanız gerekmektedir. Ürün satın almadan önce kart bilgilerinizi gireceğiniz web sitelerinin https: ile başladığından emin olmalısınız. Eğer yalnızca http: ile başlıyorsa o siteden kesinlikle alışveriş yapmamalısınız. Burada sonda bulunan “S” ifadesi secure yani güvenli anlamına gelmektedir.

8. Ne Yazdığınıza Dikkat Edin

İnternette bir silme anahtarı yoktur yani sizin internet üzerinde paylaştığınız tüm yorumlar, resimler ve içerikler silseniz dahi internet üzerinde sonsuza dek kalabilirler. Dolayısıyla içerik paylaşırken ailenizin, potansiyel işvereninizin ve geri kalan çevrenizin görmesini istemeyeceğiniz şeyler paylaşmamaya özen gösterin.

9. Kiminle Tanıştığınıza Dikkat Edin

Çevrim içi olarak tanıştığınız kişiler, her zaman iddia ettikleri kişiler olmayabilir. Hatta gerçek kişiler bile olmayabilirler. InfoWorld raporlarına göre, sahte sosyal medya profilleri sıradan sosyal medya kullanıcıların kullandığı bir yöntem olduğu kadar hackerler için de insanların hesaplarını çalmak amacıyla kullandıkları popüler bir yoldur.

10. Virüs Koruma Programınızı Güncel Tutun

İnternet güvenlik yazılımlarınız sizi her tehdide karşı koruyamayacaktır, ancak bu yazılımları güncel tuttuğunuz müddetçe sizi birçok malware virüslerinden koruyacaklardır. Dolayısıyla, işletim sisteminizin ve kullandığınız başta güvenlik yazılımlarınız olmak üzere tüm uygulamaların güncellemelerini aksatmadan düzenli bir şekilde yapmalısınız.

Eğer yukarıda bahsettiğimiz bu 10 temel internet güvenliği kuralını aklınızda bulundurup dikkatlice internette dolaşırsanız güvenlik sorunlarının çoğunu önleyeceğinizden emin olabilirsiniz.

Hazırlayan	Onaylayan
Kalite Yönetim Ekibi/ Müdür Yardımcısı Derya KARAHAN	Kalite Yönetim Temsilcisi / Müdür Ramazan ÖZYURT