İnternet üzerinden yapılan saldırılar genelde kullanıcıları yanıltmaya odaklanır. Dolandırıcılar tarafından gönderilen, bilinen bir kişi veya kurumdan geliyormuş gibi görünen e-posta veya web sayfası yoluyla kimlik bilgileri, kredi kartı/banka hesap bilgileri, kullanıcı şifre bilgilerini güncellemeniz istenir. Bilgi güncellemesi yapılan alan, sahte e-posta adresi veya web sitesi üzerindedir. Bu noktada iletilen linkte yazan adres ile link üzerine geldiğinizde görünen adresin birbiriyle aynı olmasına dikkat edilmelidir. Kullanıcı bu bilgileri aslına çok benzeyen sahte form ve web sitelerine girdiği anda bu bilgilerin çalınması riskiyle karşı karşıya kalır.

Genel olarak internet üzerinden yapılan saldırılara karşı alabileceğiniz güvenlik önlemleri şunlardır:

- Bilgisayarınızda bir anti virüs programı kullanın ve güncellemelerini yapmayı ihmal etmeyin.
- Tanımadığınız kişilerden gelen e-postaları dikkate almayın ve açmayın. Bazen bu mailleri sadece açmak bile bilgisayarınıza virüs bulaşmasına sebep olabilir.
- E-posta yoluyla gelen her web site adresine tıklamayın, girmek istediğiniz web sitesinin adresini, adres barına kendiniz yazarak girin.
- Şüpheli ve güvensiz görünen ağlardan elektronik işlem gerçekleştirmeyin.
- Bilmediğiniz, şüpheli veya güvenli görünmeyen sitelerden dosya indirmeyin.

Bazı dolandırıcılar telefonla sizi arayarak kendilerini avukat, polis, savcı, bankacı veya şirketimiz çalışanı gibi tanıtabilir ve sizden kredi kartınızın şifresi ya da SMS ile gelen şifreleri isteyebilir. Bu tip bilgilerinizi, şirketimiz personeli dahi olsa, kimse ile paylaşmayınız.