**فیشینگ وب (Web Phishing)**

**فیشینگ وب** یکی از رایج‌ترین روش‌های حملات سایبری است که در آن هکرها تلاش می‌کنند کاربران را فریب دهند تا اطلاعات حساس و شخصی خود، مانند نام کاربری، رمز عبور، شماره کارت بانکی یا اطلاعات مالی را افشا کنند. این حمله معمولاً از طریق وب‌سایت‌های جعلی یا لینک‌های مخرب انجام می‌شود که به گونه‌ای طراحی شده‌اند که شبیه وب‌سایت‌های معتبر به نظر برسند.

**1) روش‌های اجرای فیشینگ وب**

**ایجاد وب‌سایت جعلی**

مهاجم یک وب‌سایت تقلبی ایجاد می‌کند که بسیار شبیه به وب‌سایت رسمی یک سازمان معتبر (مانند بانک، شبکه‌های اجتماعی یا فروشگاه‌های آنلاین) است.

**ارسال لینک‌های مخرب**

هکرها از طریق ایمیل، پیامک یا پیام‌های شبکه‌های اجتماعی لینک‌هایی را ارسال می‌کنند که کاربران را به وب‌سایت‌های جعلی هدایت می‌کنند.

**نمایش پیام‌های اضطراری**

فیشینگ اغلب با نمایش پیام‌هایی مثل "حساب شما مسدود شده است" یا "نیاز به تأیید فوری اطلاعات" همراه است تا کاربران سریعاً واکنش نشان دهند.

**2) ویژگی‌های وب‌سایت‌های فیشینگ**

**آدرس وب‌سایت مشابه اما متفاوت**

وب‌سایت‌های فیشینگ معمولاً از دامنه‌هایی استفاده می‌کنند که شبیه به وب‌سایت اصلی هستند اما شامل تغییرات کوچک مانند اضافه کردن یک کاراکتر یا تغییر دامنه (مثلاً .com به .net) هستند.

**عدم وجود HTTPS**

اکثر وب‌سایت‌های جعلی از پروتکل امن HTTPS استفاده نمی‌کنند و در نوار آدرس مرورگر، نماد قفل وجود ندارد.

**طراحی ظاهری مشابه**

طراحی وب‌سایت‌های فیشینگ ممکن است کاملاً مشابه وب‌سایت اصلی باشد تا کاربران متوجه تفاوت نشوند.

**3)روش‌های محافظت در برابر فیشینگ وب**

**دقت در بررسی آدرس وب‌سایت**

قبل از وارد کردن اطلاعات، آدرس وب‌سایت را با دقت بررسی کنید و از صحت آن مطمئن شوید.

**استفاده از گواهینامه‌های امنیتی**

وب‌سایت‌های معتبر از پروتکل HTTPS و گواهینامه SSL استفاده می‌کنند.

**عدم کلیک روی لینک‌های ناشناس**

از کلیک روی لینک‌های ارسال‌شده توسط افراد یا ایمیل‌های ناشناس خودداری کنید.

**فعال‌سازی احراز هویت دو مرحله‌ای**

این روش امنیت حساب‌های کاربری را افزایش می‌دهد و دسترسی غیرمجاز را سخت‌تر می‌کند.

**استفاده از نرم‌افزارهای آنتی‌ویروس**

آنتی‌ویروس‌های معتبر می‌توانند لینک‌های مخرب و وب‌سایت‌های جعلی را شناسایی کنند.

**4)عواقب حملات فیشینگ وب**

**سرقت اطلاعات مالی**

هکرها از اطلاعات به‌دست‌آمده برای برداشت غیرمجاز پول از حساب بانکی قربانیان استفاده می‌کنند.

**هک حساب‌های کاربری**

اطلاعات سرقت‌شده می‌توانند برای ورود به حساب‌های ایمیل، شبکه‌های اجتماعی یا سایر خدمات آنلاین استفاده شوند.

**سوءاستفاده هویتی**

اطلاعات شخصی ممکن است برای جعل هویت و انجام فعالیت‌های غیرقانونی مورد استفاده قرار گیرد.

**نتیجه‌گیری**

فیشینگ وب یکی از جدی‌ترین تهدیدهای امنیت سایبری است که به دلیل سادگی اجرا و میزان تأثیرگذاری بالا، به طور گسترده توسط هکرها استفاده می‌شود. افزایش آگاهی کاربران، توجه به نکات امنیتی و استفاده از ابزارهای حفاظتی می‌تواند به کاهش خطرات ناشی از این حملات کمک کند.