پنجشنبه 07 آذر 1387 - 08:41

آشنایی با حملات فیشینگ

همشهری آنلاین:

حملات فیشینگ (Phishing) عبارت است از ترغیب کاربران به افشای اطلاعات محرمانه شخصی با استفاده از هویت‌های قلابی و ساختگی.

حملات فیشینگ معمولاً در قالب‌های زیر ظاهر می‌شوند:

- ایمیل از طرف فردی که ادعا می‌کند دوست یا همکار شما است.
- پیغام یا تبلیغ در شبکه‌های اجتماعی
- وب‌سایتی قلابی که که برای امور خیریه تقاضای کمک می‌کند.
- وب‌سایتی با نامی مشابه وب‌سایت‌هایی که شما متناوباً به آن‌ها سر می‌زنید.
- در برنامه‌های پیغام فوری مانند یاهو مسنجر یا ویندوز لایو مسنجر
- از طریق پیام‌های کوتاه تبلیغاتی بر روی تلفن همراه شما

این حملات شکل‌هایی نظیر درخواست اطلاعات از سوی بانکی قلابی، اعلام برنده‌شدن شما در قرعه‌کشی و یا پیغامی از طرف شبکه‌های اجتماعی به خود می‌گیرند.

ایمیل‌های فیشینگ معمولاً دارای لوگوها و تیترهای رسمی از بانک‌ها یا موسسات مالی معتبر هستند و حاوی درخواست ارائه اطلاعات شخصی و حساس هستند.

سازندگان این ایمیل‌ها معمولاً برای رسمی جلوه‌دادن بیشتر فعالیت‌های خود، لینکی از سایتی با ظاهری آراسته و رسمی به ایمیل‌های خود اضافه می‌کنند.

برای ایمن کردن خود در برابر حملات فیشینگ بهترین و کامل‌ترین راه، استفاده از ویروس‌یاب‌ها و برنامه‌های امنیتی به روز است.

بعضی از ایمیل‌های فیشینگ حاوی فایل‌ها و برنامه‌های مخرب نیز هستند به همین دلیل یکی از بهترین راه‌ها برای مقابله با آن‌ها به روز سازی نرم‌افزارهای امنیتی است.

در بعضی از نسخه‌های مرورگرهای وب برنامه‌هایی به عنوان فیلتر مطالب ناخواسته یا سایت‌های غیر معتبر وجود دارد. این نرم‌افزارها اطلاعات سایت‌هایی را که از مجوزهای SSL استفاده می‌کنند به نمایش می‌گذارد و لایه‌ای امنیتی برای کاربران ایجاد می‌کند.