

مزایا و معایب بانکداری الکترونیک

مزایای بانکداری الکترونیک

از آنجا که ارگان های که با بانک به صورت مستقیم در ارتباط هستند به دو دسته از جمله موسسات مالی و مشتریان هستند پس از دید این دو، مزایا را مورد بررسی قرار داده ایم.

از دید موسسات مالی: ایجاد و افزایش شهرت بانکها در ارائه افزایش نوآوری، حفظ مشتریان علی رغم تغییرات مکانی بانکها، ایجاد فرصت برای جستجوی مشتریان جدید در بازارهای هدف، گسترش محدوده جغرافیایی فعالیت و برقراری شرایط رقابت کامل را نام برد.

از دید مشتریان: صرفه جویی در زمان، صرفه جویی در هزینه ها و دسترسی به کانال های متعدد برای انجام عملیات بانکی نام برد.

بر اساس تحقیقات موسسه Data Monitor مهم ترین مزایای بانکداری الکترونیک عبارتند از: تمرکز بر کانال های توزیع جدید، ارائه خدمات اصلاح شده به مشتریان و استفاده از راهبردهای تجارت الکترونیک. البته مزایای بانکداری الکترونیک از دیدگاه های کوتاه مدت، میان مدت و بلند مدت نیز قابل بررسی است. رقابت یکسان، نگهداری و جذب مشتریان از جمله مزایای بانکداری الکترونیک در کوتاه مدت (کمتر از یکسال) هستند. در میان مدت (کمتر از ۱۸ ماه) مزایای بانکداری الکترونیک عبارتند از: یکپارچه سازی کانالهای مختلف، مدیریت اطلاعات، گستردگی طیف مشتریان، هدایت مشتریان به سوی کانال های مناسب با ویژگی های مطلوب و کاهش هزینه ها، کاهش هزینه پردازش معاملات، ارائه خدمات به مشتریان بازار هدف و ایجاد در آمد نیز از جمله مزایای بلند مدت بانکداری الکترونیک هستند.

معایب بانکداری الکترونیک:

مشتری برای بهره مند شدن از مزایای بانکداری الکترونیک باید به کامپیوتر دسترسی داشته باشند.

مهمترین مشکل مربوط به مقوله امنیت می باشد.

امنیت:

اساساً دو روش امنیتی متفاوت برای بانکداری آنلاین وجود دارد :

سیستم PIN/TAN که PIN نشان دهنده یک رمز عبور برای ورود است و TAN نشان دهنده رمزهای عبور یکبار مصرف است که برای اعتباربخشی و امنیت تراکنش هاست. TANها به شیوه‌های گوناگونی توزیع می‌شوند که معمولترینش اینست که یک لیست از TANها توسط نامه پستی به کاربر بانکداری آنلاین فرستاده می‌شود. امن‌ترین راه استفاده از TANها اینست که آنها رو بر حسب نیاز توسط یک نشان امنیتی تولید کنیم معمولاً بانکداری آنلاین با PIN/TAN از طریق مرورگرهایی که از ارتباطات امن SSL استفاده می‌کنند انجام می‌شود بنابراین نیازی به رمزنگاری اضافه‌ای نیست. حملات بیشتر حملات به بانکداری آنلاین امروزه بر پایه فریب کاربر برای دزدیدن اطلاعات ورود و TANهای معتبر است. یک مثال شناخته شده برای این حملات ساخت صفحه مشابه یک سایت برای فریب کاربر است تا با وارد کردن اطلاعات شخصی خود آنها را در اختیار دزدان قرار دهد. همچنین نوشتن اسکریپت سایت های عبور و یا استفاده از ضبط کننده‌های کیبورد (تروجان ها) هم به عنوان راه‌هایی برای سرقت اطلاعات افراد به کار می‌رود. یک روش برای حمله به بانکداری آنلاین مبتنی بر امضا اینست که نرم افزار مورد استفاده را جوری دستکاری کنند که روی صفحه نمایش تراکنش صحیح را نشان دهد ولی در پشت صحنه، یک تراکنش دروغین امضا شود. گزارش اخیر تکنولوژی FDIC که از گردآوری و همگردانی گزارش فعالیت فایل‌های مشکوک بانک ها، هر ۳ ماه یکبار تشکیل می‌شود، ۵۳۶ مورد جرائم رایانه‌ای را لیست کرده که به طور میانگین، هر کدام باعث ۳۰۰۰۰ دلار ضرر شده است. این رقم در چارک دوم سال ۲۰۰۷ به ۱۶ میلیون دلار افزایش یافته است. تخلفات رایانه‌ای بین چارک اول و دوم سال ۲۰۰۷ - ۱۵۰ درصد افزایش داشته است. گزارش ها حاکیست در ۸۰ درصد موارد منبع تجاوز نامعلوم است ولی در حین بانکداری آنلاین انجام گرفته است.

اقدامات متقابل اقدامات متقابل زیلدی وجود دارند که سعی می‌کنند از تجاوز جلوگیری کنند. گواهینامه دیجیتال برای مقابله با صفحات مشابه دروغین به کار می‌روند، استفاده از کارتخوان های گروه ۳ تلاشی برای جلوگیری از دستکاری تراکنش ها به وسیله نرم افزار در انواع روش های بانکداری آنلاین مبتنی بر امضا است. برای محافظت سیستمشان از تروجان ها، کاربران باید از نرم افزارهای تشخیص دهنده ویروس استفاده کنند و مراقب نرم افزارهای داندودی و فایل های پیوستی به ایمیل ها باشند. در سال ۲۰۰۱ موسسه FFIEC راهنمای تشخیص هویت چندمعیاره (MFA) را منتشر کرد و از آن پس، تا اواخر ۲۰۰۶ نیاز به حضور در محل بود.

منبع:

www.DataMonitor.com