جرایم سایبری

در شماره قبل ماهنامه مطلبی با عنوان جرایم اینترنتی یا سایبری ارائه شد. اکنون در ادامه این بحث و در این قسمت به جای پرداختن به چند مطلب از شاخه های مختلف رشته حقوق و جرایم سایبری، یکی از خدمات اینترنت به طور خاص و فضای سایبری به طور عام را با رویکرد با مسائل جزایی، پیشگیری و فنی معرفی می کنیم و زمینه ای را برای ورود خوانندگان محترم و قضات به مباحث عملی در کنار مطالب تئوری فراهم می آوریم. این مقاله به قلم محمد حسن دزیانی نوشته شده است.

■ پست الکترونیک

پست الکترونیک را می توان از سه منظر یا دیدگاه مورد بحث قرار داد. نخستین جنبه که بر دو جنبه یا دیدگاه دیگر اثر فراوان دارد جنبه یا دیدگاه فنی است قطعاً شناخت فنی یک خدمت، وسیله، واسط و . . . در درک حقوقی و جزایی پدیده های ناشی از آن . . . بیشترین اثر را دارد. جنبه دیگر، جنبه جزایی و در آخر جنبه سوم، جنبه حقوقی پست الکترونیک است. در این مقاله فقط برای طرح بحث و فراهم آوردن زمینه ورود برای خدمت نکات کلی را عنوان و تفصیل آن را به متون تفصیلی واگذار می کنیم.

الف - جنبه فنی

برای شناخت ابتدایی پست الکترونیک از جنبه فنی، پرداختن به چند نکته لازم به نظر می رسد: مکان، اهمیت، روش کار و . . .

۱ - امکان:

پست الکترونیک یا به طور رایگان توسط برخی موتورهای جستجو ارائه می شود یا با پرداخت هزینه قابل دسترس است. موتورهای جستجو مانند یاهو و گوگل به طور رایگان این خدمت را ارائه می کنند و حجم قابل توجهی را در اختیار کار برقرار می دهند. یاهو به تبعیت از وعده و وعیدهای گوگل اخیراً حجم پست الکترونیک را افزایش داده و تا ۲۵۰ مگا بایت فضا در اختیار کار برگذاشته است. درکنار یاهو و گوگل برخی مراجع دیگر مانند هات میل، اوت لوک و . . . خدمات پست الکترونیک را ارائه می کنند. برخی سازمانهای دولتی و بخش خصوصی به تبع سایت یا مرکز مرور خود، خدمات پست الکترونیک به هر کارمند خود واگذار می کنند که البته بیشتر کاربرد اداری دارد که در بکارگیری آن باید دقت بیشتری کردو برخی دهندگان خدمات اینترنت (ISP) نیز بر اساس اکانت واگذاری به کاربر، خدمات پست الکترونیک ارائه می کنند که البته هزینه آن همراه با اکانت کلی کاربری محاسبه می شود. تفاوت مراجع یاد شده در نوع کاربری، هزینه اقتصادی، امنیت کاربری و . . . است. طبعاً با بالا رفتن میزان حساسیت فعالیت کاربر، توجه به مرجع دریافت کننده خدمت پست الکترونیک باید بیشتر شود.

۲ - اهمیت:

در خصوص اهمیت پست الکترونیک از جنبه غیر حقوقی می توان گفت کاربری این خدمت نسبت به پست معمولی ارزان تر، سریع تر و تا حد زیادی مطمئن تر می باشد. پست یک نامه علاوه بر زمانی که ارسال و دریافت آن می طلبد مستلزم هزینه های بعضاً قابل توجه و زیاد است اما پست الکترونیک چنین نیست. در نظر بگیرید اگر با مثالی بخواهیم تفاوت این دو نوع ارسال و دریافت پیام را تبیین کنیم می توانیم بگوییم اگر یک نامه معمولی حدود پانصد تومان هزینه در برداشته باشد ارسال یک نامه الکترونیکی حدود پنجاه تومان هزینه دارد و از لحاظ ارسال و دریافت (بعد زمانی) اگر یک نامه بدون بروز حوادث و بلایای طبیعی و غیر طبیعی ۲ یا ۳ روزه به دست مخاطب و گیرنده می رسد پست الکترونیک به محض ارسال یا با چند ثانیه تأخیر توسط دریافت کننده قابل دریافت و قابل مرور است.

اما این بعد سرعت ارزانی ما را متوجه امر دیگری می کند و آن امنیت است. خدمات رایگان در درگیری امنیتی بیشتر در فضای سایبر دارند زیرا انواع اسپیم (پیام ناخواسته)، نفوذگری و . . . آنها را در معرفی تهدید و خطر قرار می دهند. پزشکی که برای اعمال جراحی مهم منتظر پست الکترونیک است، نباید خدمات ایمیل خود را از یک مرجع رایگان عام مانند یاهو و . . . دریافت کند چرا که این امر مشکلات زیادی را بر دارد. همچنین برای تنظیم جلسات کاری مهم و . . . باید به این مهم

توجه داشت.

اما اهمیّت پست الکترونیک از جنبه حقوقی بسیار زیاد و چشمگیر است. حقوقدانان به این خدمت اینترنتی بعنوان یک ابزار کار یا موضوع کشف علمی جرایم سایبری، جرایم سایبری (جزای اختصاصی)، تحقیقات جنایی (مقدماتی) جرایم سایبری و پیشگیری نگاه می‌کنند. درکنار اهمیت فوق‌العاده جزایی، از نظر حقوقی در بحث عقود و تعهدات حقوق بین‌الملل خصوصی، تجارت الکترونیک و بانکداری الکترونیک پست الکترونیک واجد اهمیت زیادی است. در ادامه همین نوشتار به طور خلاصه به این مطالب اشاره خواهیم کرد.

۳- باز کردن:

برای باز کردن یک پست الکترونیک در موتور جستجویی مانند یاهو باید روی نمادی یا آیکون پست الکترونیک (ایمیل) در صفحه اصلی این موتور جستجو کلیک کرد. پس از باز شدن صفحه پست الکترونیک سه حالت مشاهده می‌شود دو مورد مستلزم پرداخت هزینه و یک مورد رایگان (Free) است.

روی مورد رایگان کلیک کنید صفحه‌ای باز می‌شود که حاوی پاره‌ای اطلاعات درخواستی از شما برای باز کردن یک حساب برای شمااست. لزومی ندارد همه سؤالات اطلاعات درست و منطبق با واقع باشد اما اگر درست باشد بهتر است (استثناء: افراد نظامی، افراد دارای شغل مهم، کسانی که به هر دلیلی قصد ناشناس ماندن دارندو البته خلافکاران). معمولاً اطلاعات درخواستی شامل اسم، فامیل، اسم مدرسه، اسم سگ یا گربه در صورت وجود، تاریخ تولد، کد کشور (این یک را با اعداد غیردقیق مانند ۱، ۲، ۳، ۴ و ... پر کرد)، انتخاب موضوعات مورد علاقه جهت دریافت مطالب و ... می‌باشد. در انتخاب موضوعات مورد علاقه و نیز اینکه دوست دارید آدرس شما در اختیار دیگران قرار گیرد یا خیر، دقت کنید. علت دقت به این نکات، دوری از اسم، اجتناب از نفوذ افراد ناشناس، پرشدن ایمیل به صورت ناخواسته و یا مطالب نامربوط و ... است. معمولاً برای انتخاب آدرس، اسم به علاوه علامت ات ساین و یاهو دات کام ذکر می‌شود اسم نباید از اسامی شایع یا قبلاً استفاده شده باشد. از انتخاب اسامی ساده بپرهیزید و سعی کنید اسم ترکیبی از حروف و علایم یا اعداد باشد. طبعاً یاهو در صورت تکراری بودن اسم یا وجود برخی نمادها آن را نمی‌پذیرد.

با اتمام کار و پذیرش شمادر یاهو، پست الکترونیکی از طرف یاهو مبنی دایر بر خوش آمد گویی و اینکه دارای پست الکترونیک شده‌اید دریافت خواهید کرد. گذر واژه و نام کاربردی خودرا فراموش نکنید و اگر به حافظه خود اطمینان ندارید این دو را در جایی یادداشت کنید. البته خود صفحه آغازین به پست الکترونیک نیز این امکان را برای شما فراهم می‌آورد.

۴- مرور پست الکترونیک:

در اینجا نیز مثالی از یاهو می‌زنیم. زمانی که آدرس ایمیل را در یاهو داشته باشید یا به اصطلاح ثبت شده باشید، با کلیک روی نماد پست الکترونیکی در صفحه آغازین یاهو می‌توانید به صفحه ایمیل وارد شوید و سپس با ورود گذر واژه و نام کاربردی و کلیک روی قسمت مربوط به صفحه پست الکترونیک خود وارد شوید برای مرور نامه‌ها و پیام‌ها از چک میل استفاده کنید یا روی اعداد نشانگر پیامهای ارسالی برای شما کلیک کنید. برای دیدن هرنامه یا پیام روی آن کلیک کنید و پس از مرور آن را ببندید(back). می‌توانید در صورت نیاز از آرشیو برای نگهداری متن و از آدرس بوک برای نگاهداری آدرس ها استفاده کنید.

برای ارسال ایمیل از compose و برای پاسخ به فردی که از او نامه ای دریافت کردید از reply و برای ارسال متن به دیگریان از خود وارد استفاده کنید. در صورت نیاز می‌توانید فایلهایی را به متن نامه خود پیوست کنید.

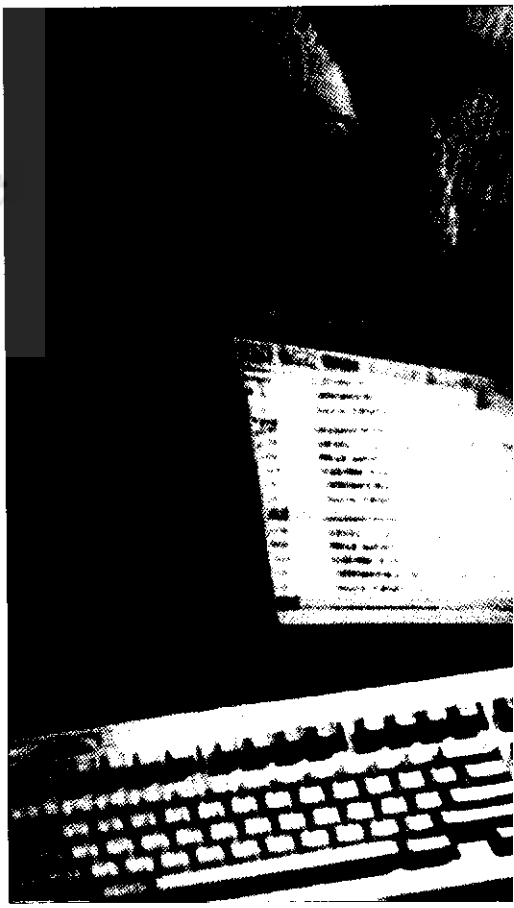
همواره به خاطر داشته باشید پس از اتمام کار با صفحه‌ای میل خود آن را ببندید (sign out). باز گذاشتن این صفحه به معنای باز بودن در به روی هر ناشناس و غریبه است و امکان مرور نامه‌های شما وجود خواهد داشت. لزوم بستن ایمیل (فقط از طریق sign out) جزء نکات امنیت اینترنت و سیستم است که باید نسبت به آن دقت کنید.

۵- توصیه‌های فنی:

قبل از ورود به مباحث جزایی و حقوقی بد نیست نکات فنی را متذکر شویم چرا که در با مباحث جزایی و حقوقی مرتبط است و اهمیت زیادی دارد. روی دیگر سکه توصیه‌های فنی، مسائل کشف علمی و پیشگیری جرایم سایبر و ... قرار دارد. عدم دقت به برخی مسائل فنی گاه موجب تحقق مسؤولیت کیفری و ... است.

- از باز کردن موارد مشهور به بالک (balk)، فایلهای دارای پسوند اگزه (exe) و پیامهای ناشناس بپرهیزید علت این امر نیز مشخص است یا در معرض پیام ناخواسته قرار خواهید گرفت یا به ویروس مبتلا خواهید شد یا آدرس شما برای مجرمان سایبری مشخص خواهد شد.
- هرگز به پیام ها و نامه‌های الکترونیک حاوی فحاشی، تهدید، سؤالات مبهم و ... پاسخ ندهید (reply). با اینکار آدرس و مشخصات کاربری خود را افشا می‌کنید یا اینکه هکرهایی که بدنبال عصبانی کردن دیگران هستند موفق به عصبانی کردن شما می‌شوند یا انیکه از هویت شما آگاه خواهند شد و ...
- نامه‌ها یا پیام های الکترونیک که دریافت می‌کنید حتی‌الامکان برای دیگران ارسال نکنید (foreward)، هیچگاه از نقص امنیتی دریافت کنندگان بعدی آگاهی درستی ندارید مسیرهای ناشناخته و مشکوکی نیز وجود دارند که خطرات زیادی برای شما و دیگران ایجاد می‌کنند. ارسال به دیگران باید حتی‌الامکان بصورت موارد معدود و نادر صورت گیرد و ...
- برای پیگیری فرستنده برخی سایتها مانند (tracert) و ... وجود دارند که آدرس و مسیر ارسال پیام را مشخص می‌کنند البته این امکان همیشه وجود ندارد و فقط برخی مواقع میسر است. اگر نتوانستید آدرس فرستنده را پیگیری کنید مستقیماً به شناسایی فرستنده اقدام نکنید بلکه از تهیه کننده خدمات (IPS) خود یا مسئول سرور سایت محل کارتان کمک بگیرید.
- ایمیل خود را بی مورد به افراد ندهید گاه افراد غیر لازم آدرس ایمیل را دریافت می‌کنند. در صورت

همواره به خاطر داشته باشید پس از اتمام کار با صفحه‌ای میل خود آن را ببندید (sign out) باز گذاشتن این صفحه به معنای باز بودن در به روی هر ناشناس و غریبه است و امکان مرور نامه‌های شما وجود خواهد داشت



لزوم بسته به مورد و موضوع ارتباط از ایمیل اداری ، سازمانی یا شخصی خود استفاده کنید و آدرس را حسب موضوع بدهید . به سایتهای ناشناس و نیز سایتهای که به شغل یا فعالیت حرفه ای شما ربطی ندارند یا شناخت دقیق از آن ندارید ، آدرس ایمیل خود را ندهید .

■ وقتی به سایتی می روید که آدرس ایمیل یا نام کاربری و گذر واژه از شما می خواهد نخستین کار اجتناب از دادن آدرس یا دادن اطلاعات است اگر سایت معتبری است جوانب کار را بررسی و سپس اقدام به دادن آدرس ایمیل و . . . کنید . از پاسخ به نامه ها یا سایتهایی که آدرس ایمیل شما را برای کنترل انطباق یا عدم انطباق آدرس کنونی با آدرس موجود در پایگاه داده بپرسیزید . چرا که این عمل مقدمه نفوذ ، کلاهبرداری ، مزاحمت و . . . می باشد .

■ در خصوص بانوان و کودکان باید دقت بیشتری کرد . آدرس ایمیل برخی بانوان که برای دیدار از سایتهای به ظاهرخوب داده شده بعداً بصورت دفترچه حاوی اسامی زنان روسپی و . . . استفاده شده یا اینکه این بانوان را در معرفی دریافت نامه های حاوی فحاشی ، تصاویر پورنوگرافیک و . . . قرار داده است کودکان نیز در معرفی قاچاقچیان کودک ، پورنوگرافرها و . . . هستند . به این نکات از نظر آسیب شناسی بسیار دقت کنید .

■ در خصوص افراد نظامی وامنیتی باید گفت این افراد معمولاً ایمیل ندارند یا اینکه نباید داشته باشند و اگر دارای ایمیل باشند آدرس ایمیل و مشخصات ، کاذب است و باید دقت لازم در خصوص این افراد شود و بعضاً برخوردهای حفاظتی برای جلوگیری از سوء استفاده یا کوتاهی افراد یاد شده صورت گیرد .

■ اگر علاقمند به سرزدن به سایتهای مختلف هستید یا مبتلا به کار شما است از دو یا چند ایمیل استفاده کنید یعنی چند ایمیل درست و بسته به مورد از آدرس ایمیل های متنوع استفاده کنید . پرهیز از این کار شما را در معرض انواع پیام ناخواسته ، حجم بالای مطالب مستهجن ، حملات هکری و . . . قرار می دهد . فایده دیگر داشتن چند ایمیل این است که : به هنگام کشف علمی جرایم سایبری و نیز تحقیقات مقدماتی مطمئن شوید متهم یا مظنون یک ایمیل بیشتر نداشته باشد و اگر بیش از یک ایمیل دارد حتماً آنها را به دقت بررسی کنید . به یاد داشته باشید قاچاقچیان ، تروریستها و . . . دارای چند آدرس ایمیل هستند .

■ به خاطر داشته باشید سرزدن به برخی سایتها موجب لو رفتن اطلاعات هویتی شما ، شماره های کاربری و کدهای کامپیوتر شما و . . . می شود لو رفتن این اطلاعات مساوی است با لو رفتن مسیرها و اطلاعات سازمانی و شغلی و . . . سایت علمی یا سایت تجاری و . . . معمولاً نیاز به اطلاعات مهم و هویتی شما ندارد . اگر اطلاعاتی از این دست را از شما طلب کردند بدواً در مورد آنها بررسی و کنکاش کنید .

■ کودکان و افراد زیر ۱۸ سال و بانوان هر گاه با پیام الکترونیک حاوی فحاشی ، تصاویر مستهجن و . . . روبرو شدند باید پلیس والدین و مقامات مربوطه را مطلع کنند تا برخورد قانونی با آنها صورت گیرد .

■ هرگاه با پیام حاوی پیشنهاد کار مبتنی بر این که شما را سریعاً پولداری کند یا در آن از شما شماره حساب خواسته شده نگران حضور کلاهبرداران دسته اندرکاران پولشویی باشید . در این حال اطلاع به پلیس و مقامات قضایی بهترین واکنش است .

■ تبلیغات و پیام های ناخواسته جزء جدا نشدنی از ایمیل هستند اقلام مربوط به دریافت این تبلیغات را علامت نزنید یا درصورت لزوم از تهیه کننده خدمات خود بخواهید آنها را محدود کنند همچنین می توانند از نسخه جدیدتر ویندوز XP ، نرم افزار های ضد اسپم و . . . استفاده کنید .

به هنگام کشف علمی جرایم سایبری و نیز تحقیقات مقدماتی مطمئن شوید متهم یا مظنون یک ایمیل بیشتر نداشته باشد و اگر بیش از یک ایمیل دارد حتماً آنها را به دقت بررسی کنید

■ به یاد داشته باشید به هنگام باز کردن ایمیل ، برخی تصاویر نه چندان معقول روی هارد و ثبت و دقایع جای می گیرد . اگر بعنوان قاضی یا مدیر سیستم با این پدیده روبرو شدید اصل را بر برائت بگذارید و در صورت اثبات ورود عمدی کاربر به سایتهای خلاف اخلاق واکنش نشان دهید .

■ به یاد داشته باشید مدیر سیستم ، تهیه کنندگان خدمات (ISP) و . . . امکان مرور پیام های شما را دارند .

■ برخی قوانین مانند قانون میهن پرستی آمریکا (پاتریوت) و مقررات مشابه در آمریکا و اروپا روی برخی واژگان حساسند . از بکار بردن واژگان مبهم یا شوخی های نادرست بپرهیزید زیرا دریافت کننده پیام مستقیم آمریکا و اروپا با مزاحمت پلیس و نیروهای ویژه مواجه می شود بدون اینکه عمل منفی از او سرزده باشد .

گفتنی های فنی بیش از این موارد است اما امیدوارم با این حداقل به مشکلات مرسوم در ایمیل برنخورید . در عین حال با ذکر این مختصر نکات فنی می توان به سراغ بحث جزایی و حقوقی پست الکترونیک رفت .