

Amenazas al usuario final

¿Cómo se protege doña Rosa?



¿Por qué el usuario final se ve amenazado?

- Hoy en día, casi todos somos usuarios informáticos
- El usuario maneja información
- Muchas veces es el eslabon más débil de la cadena
 - Aplicaciones y redes tienen cada vez más protecciones
 - Red corporativa vs Uso de PC en el hogar

¿Qué buscan los atacantes?

- Robo de información
 - Claves de acceso a Home Banking / Números de tarjeta de crédito
 - Datos estadísticos (ej: Software espía)
- Utilización de recursos informáticos
 - Control de la PC por parte de atacantes (ej: BotNets)

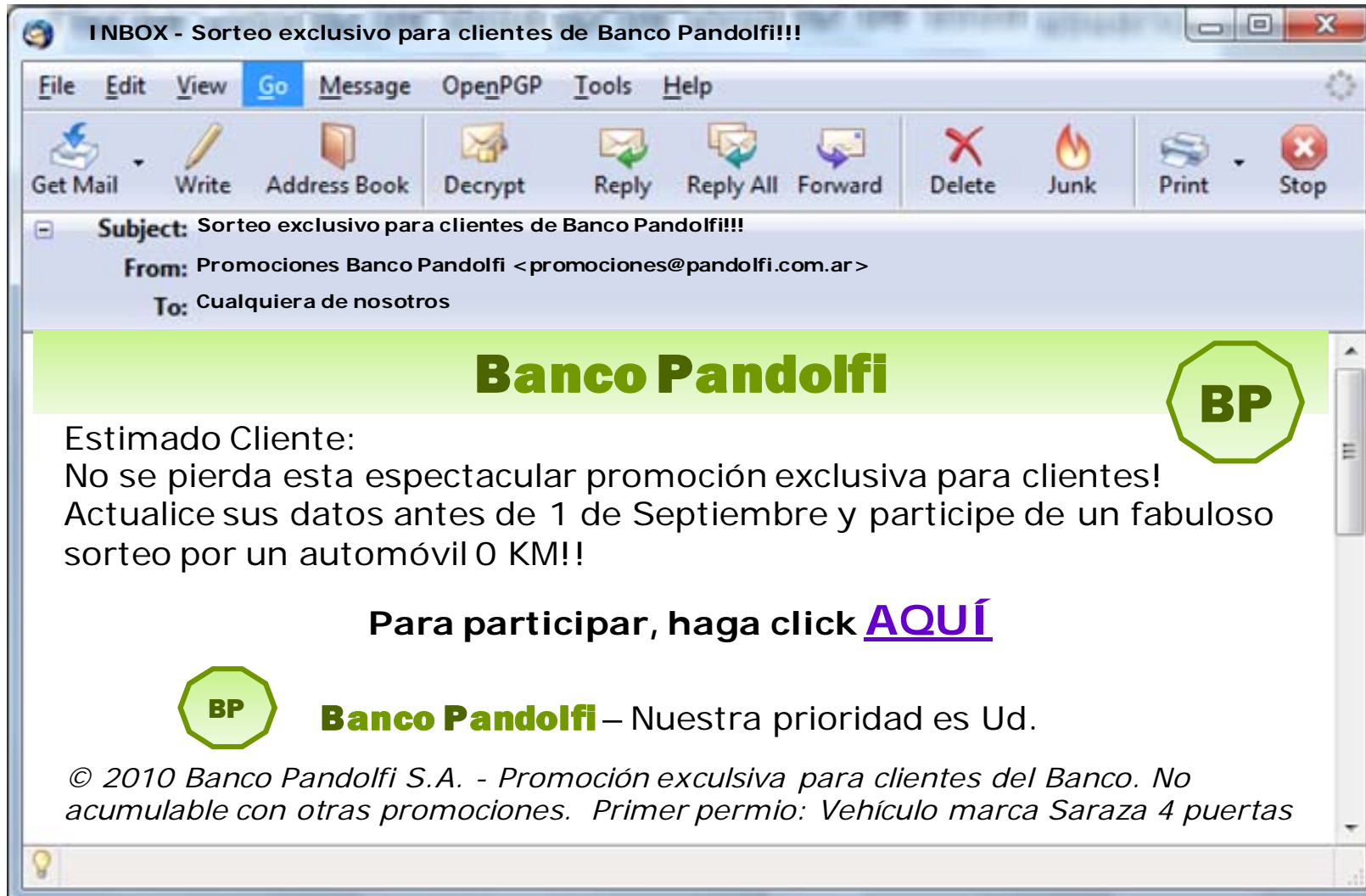
Amenazas actuales más habituales al usuario final

- Phishing
- Infección con Malware
- Robo de dispositivos móviles
 - (CON LA INFORMACIÓN ADENTRO!)
- Uso inseguro de redes inalámbricas
- Uso inseguro de redes sociales



A

Phishing (Tratando de “pescar” a la víctima)



A Phishing *(Tratando de “pescar” a la víctima)*

¿Qué es?

- Trampa destinada a engañar a los usuarios
- Usualmente vía mail
- Se suele utilizar el “look & feel” de una empresa conocida
- Por lo general, se intenta dirigir al usuario a un sitio falso.

¿Qué quiere lograr el atacante?

- Robo de credenciales
- Datos Bancarios
- Números de tarjetas de crédito
- Robo de Dinero



Mecanismos de protección

- Autenticación de 2 factores
 - Muy empleado actualmente por bancos
 - Ej: Tarjeta de coordenadas, e-token, etc
- Conciencia
 - No seguir enlaces “embebidos” en e-mails
 - Verificar la URL a la que se ingresa
 - Verificar los datos del certificado de un sitio Web (HTTPS)
 - Atender las advertencias del navegador Web (ej: inconsistencia con el nombre del certificado)
 - Extremar las precauciones antes de colocar en la Web credenciales (contraseñas) o números de tarjetas de crédito.



A Malware (Software malicioso)

¿Qué es?

“Software que se infiltra en una computadora sin el consentimiento del usuario”

Tipos de Malware

- Virus / Gusanos
- Troyanos / Puertas traseras (backdoors)
- Software Espia (Spyware) / Software publicitario (Adware)

¿Quién los inventa? ¿Cuál es la finalidad?

- Robo de información
 - Virus bancarios / Keyloggers
- Robo de recursos
- Publicidad





Malware (Software malicioso)

¿Cómo se infecta mi PC?

- Propagación de malware por USB
- Software (pirata) bajado de páginas Web
- Apertura de archivos enviados por desconocidos
- Simple navegación por sitios peligrosos
- Conectar la PC en una red donde hay otras infectadas

Mecanismos de protección

- Antivirus-AntiSpyware
- Actualizaciones de software (Parches de seguridad)
- Uso de Firewall Personal
- Configuración del equipo personal (ej: Desactivar “Autorun”)
- Conciencia!



Seguridad en notebooks y equipo móvil en general.

Motivación

- Gran popularidad de equipos informáticos móviles
 - Notebooks, Netbooks, Celulares inteligentes (SmartPhones), PenDrives, etc.
- “Facilidad” de robo
- Valor de reventa del hardware...
- ...¿Valor de la información?

¿Qué información tenemos en nuestro equipo?

- Datos personales
- Backups
- Información laboral
- Contraseñas “cacheadas”



Seguridad en notebooks y equipo móvil en general.

Mecanismos de protección

- **Encriptación de la información importante**
 - Encriptación de archivos / Unidades encriptadas virtuales
 - Encriptación a nivel de disco
 - Soluciones de encriptación para dispositivos USB
 - Gestores de contraseñas
- **Conciencia!**
 - No almacenar información que no sea necesaria
 - Evitar almacenar contraseñas

iniciar sesión

Windows Live ID:

Contraseña:

[¿Ha olvidado la contraseña?](#)

Recordarme (?)
 Recordar mi contraseña (?)

[Mostrar usuarios guardados](#)

A Problemática de las redes inalámbricas

Tendencia

- Cantidad creciente de redes inalámbricas
- Configuración hogareña de WiFi
 - Hoy, cualquiera instala un Access Point
 - Muchas veces, sin las correctas medidas de seguridad
- Sitios con acceso “libre” (Hoteles / Bares / Restaurantes)
 - ¿Cuán confiable será dicha red?
- Navegación desde diferentes dispositivos
 - Notebooks, celulares, etc.



A Problemática de las redes inalámbricas

¿Y si alguien se mete en mi red?

- Ej: Por mala configuración de encriptación
- Posibilidad de ver mi tráfico e incluso de acceder a mis equipos
- Uso de mi conexión

¿Y si me meto en la red de otro?

- No sabemos qué equipos hay en dicha red
 - Posibilidad de infección con malware vía red
- No sabemos por dónde pasa el tráfico de esa red
 - Alguien podría espiar las comunicaciones



A Problemática de las redes inalámbricas

Medidas de prevención

- En casa:
 - Utilizar encriptación fuerte en la conexión con el Access Point (WPA2)
 - Cambiar la contraseña por defecto para la consola de administración
 - Preferentemente, filtrar el acceso por dirección física de red (MAC)

- Fuera de casa:
 - Precaución al conectarse a redes públicas (ej: WiFi en un bar)
 - Confiar únicamente en encriptación “punto a punto” (ej: HTTPS)
 - Configurar el “tipo de red” a “red pública” (en Windows)
 - Mantener configuración de Firewall

A Redes Sociales

Tendencia

- Las redes sociales, son espacios virtuales de interacción entre personas.
- Crecimiento y adhesión vertiginosos.
 - Hoy, casi todos tenemos un perfil en alguna red social
- Fueron diseñadas para compartir información
 - Personal / de amistades y grupos (ej: Facebook / Orkut)
 - Laboral y académica (ej: LinkedIn)
 - Comentarios breves de índole general (Twitter)



A Riesgos de las redes sociales

¿Qué información ponemos en las redes sociales?

- **Datos personales**
 - Nombres y fotos de familiares y mascotas
 - Lugares en los que estuvimos
 - Nombres de contactos y amigos
 - Comentarios diversos
- **Datos laborales**
 - Empresas en las que trabajamos actualmente y en el pasado

¿Qué pueden ver los demás de nosotros?

- Probablemente, todo lo que pusimos (x defecto todo abierto)
- Más de lo que pusimos (mis amigos, amigos de mis amigos, contactos, etc.)

A Riesgos de las redes sociales

Casos reales

- El sitio “*pleaserobme.com*” utilizaba servicios de twitter para decir que personas estaban fuera de su casa.
- Caso de Sarah Palin
 - (Reseteo de password de “yahoo mail” usando información personal el Internet)
- Otros usos malintencionados
 - Ej: Secuestros virtuales con info sacada de las redes sociales

Medidas de prevención

- Tomar conciencia de la información que se divulga
- No definir nuestras contraseñas con datos que se puedan obtener de lo que compartimos en redes sociales.
- No mantenerse afuera, pero ser precavido con la información que se provee.

A Conclusiones

- No es necesario ser experto en informática para prevenirse de los riesgos asociados con la seguridad de la información
- La conciencia es el arma principal para prevenir la mayoría de las amenazas a usuarios informáticos.
- No hay que tener miedo. El uso adecuado de los recursos informáticos es seguro.



Muchas gracias por su atención

Para mayores informaciones pmilano@cybsec.com

