Cómo proteger su información personal en linea

Contraseñas seguras

- Las cuentas más confidenciales requieren contraseñas más seguras
- Cuanto más largo sea, mejor
- Use oraciones familiares, como una línea de una canción o libro

Spam y phishing

- El spam es un correo electrónico no deseado enviado por extraños
- Marcar el spam como “basura” o “spam” permite a los filtros a reconocer mensajes similares cómo spam y enviarlos directamente a su carpeta de spam
- El phishing es un intento de robar la identidad de alguien por correo electrónico o sitio web
- “Smishing” es “phishing” mediante sms (mensajes de texto)
- No haga clic en enlaces en un correo electrónico que encuentre sospechoso
- Reenviar mensajes de texto sospechosos al 7726 (“SPAM”) de manera gratuita
- Recomendaciones de la FTC (su abreviatura en inglés “Comisión Federal de Comercio”): onguardonline.gov

Señales indicadoras de phishing

- Extraños enlaces incrustados en correos electrónicos o sitios web desconocidos
- Solicitudes de información personal y errores tipográficos o otros errores obvios
- Correos electrónicos que crean un sentido de urgencia

Compras segura en el Internet

- Busque siempre la “s” en “https” y el símbolo del candado

Mejores prácticas para redes sociales

- Nunca dé información sensible a través de redes sociales
- Ajuste su configuración de privacidad
- Evite vincular diferentes cuentas de redes sociales
- Siempre cierre la sesión cuando use una computadora pública o WiFi pública