



ACADEMIA DISCÍPULOS DE CRISTO DE BAYAMÓN

Apartado 1947

Bayamón, Puerto Rico 00960-1947

www.academiadiscipulos.com

Unidad 3: Consejos de Ciberseguridad

Objetivos de Aprendizaje:

- Conocer y aplicar consejos prácticos de ciberseguridad para proteger la información personal y profesional.
- Identificar y mitigar riesgos cibernéticos comunes.
- Fomentar hábitos seguros en el uso de dispositivos y plataformas digitales.

Contenido:

1. Contraseñas Seguras

- **Creación de Contraseñas Fuertes:**
 - Longitud mínima de 12 caracteres.
 - Uso de combinaciones de letras mayúsculas, minúsculas, números y símbolos.
- **Gestores de Contraseñas:**
 - Herramientas recomendadas como KeePass y LastPass.
 - Beneficios de usar gestores de contraseñas para almacenar y generar contraseñas seguras.

2. Autenticación Multifactor (MFA)

- **Importancia de MFA:**
 - Añadir una capa extra de seguridad a las cuentas.
 - Métodos comunes: SMS, aplicaciones de autenticación, y hardware tokens.
- **Configuración de MFA:**
 - Guía paso a paso para habilitar MFA en cuentas populares como Google, Facebook, y Microsoft.

3. Actualización Regular de Software

- **Actualizaciones de Seguridad:**
 - Importancia de mantener el sistema operativo y las aplicaciones actualizadas.
 - Configuración de actualizaciones automáticas.
- **Parcheo de Vulnerabilidades:**
 - Explicación de cómo las actualizaciones ayudan a cerrar brechas de seguridad conocidas.

4. Uso Seguro de Redes Wi-Fi

- **Redes Wi-Fi Públicas:**
 - Riesgos de conectarse a redes Wi-Fi públicas.
 - Uso de VPNs (Virtual Private Networks) para proteger la conexión.
- **Configuración Segura de Redes Domésticas:**
 - Cambiar credenciales predeterminadas del router.
 - Usar encriptación WPA3.

5. Reconocimiento y Manejo de Phishing

- **Identificación de Correos Electrónicos Sospechosos:**
 - Señales de alerta: enlaces sospechosos, errores gramaticales, remitentes desconocidos.
-
- **Acciones a Tomar:**
 - No hacer clic en enlaces ni descargar archivos adjuntos.
 - Reportar correos sospechosos a IT o a servicios de correo electrónico.

6. Copia de Seguridad (Backup)

- **Importancia del Backup:**
 - Protección contra pérdida de datos por fallos del sistema, ataques de ransomware, o eliminación accidental.
- **Métodos de Backup:**
 - Almacenamiento en la nube vs. almacenamiento local.
 - Frecuencia recomendada para realizar copias de seguridad.

7. Educación y Conciencia Continua

- **Mantenerse Informado:**
 - Suscripción a boletines de ciberseguridad y seguir a expertos en redes sociales.
- **Participación en Cursos y Talleres:**
 - Importancia de la formación continua en temas de ciberseguridad.

Actividades:

- **Video Tutorial:** Presentación sobre cómo crear y gestionar contraseñas seguras utilizando gestores de contraseñas.
- **Lectura Asignada:** Artículo sobre la importancia de las actualizaciones de software y cómo configurarlas.
- **Discusión en Grupo:** Debate sobre experiencias personales relacionadas con ataques de phishing y cómo se resolvieron. Esto se puede realizar en un foro abierto por su maestro en Microsoft Teams.

Evaluación:

- **Quiz:** Evaluación de los conocimientos adquiridos sobre los consejos de ciberseguridad y su aplicación práctica. Este quiz lo puedes encontrar en la sección de Seguridad Cibernética de la página de ADC. Enlace:
<https://quizizz.com/embed/quiz/665dc594b44cbb39ee8b2817>