Módulo 1 – Bienvenida e Introducción

La cibersegida es el conjunto de medidas y hábitos que protegen nuestra información digital frente a ataques y fraudes. No es solo para empresas: todos somos objetivos de ciberdelincuentes. Ejemplos de incidentes comunes incluyen robos de cuentas de redes sociales, fraudes bancarios por correos falsos y pérdida de fotos familiares por malware. Este curso te ayudará a aprender hábitos simples que incrementan tu seguridad digital.

Módulo 2 – Protege tus cuentas

Las contraseñas son la primera barrera de defensa. Deben ser largas (mínimo 12 caracteres), únicas y difíciles de adivinar. Evita usar fechas de nacimiento o la misma clave en varias cuentas. Para manejar múltiples contraseñas, utiliza gestores como Bitwarden o KeePass. Además, activa la verificación en dos pasos (2FA) en tus cuentas de correo, redes sociales y banca para añadir una capa extra de seguridad.

Módulo 3 – Cuidado con el phishing y las estafas

El phishing es un fraude en el que delincuentes se hacen pasar por entidades legítimas para robar datos. Señales de alerta: remitentes sospechosos, mensajes con urgencia, errores de redacción y enlaces que no coinciden con la web oficial. También existen variantes como smishing (SMS) y vishing (llamadas). Si sospechas de un mensaje, no hagas clic y accede directamente al servicio desde su web oficial. Si caes en el engaño, cambia contraseñas, activa 2FA y avisa a tu banco.

Módulo 4 – Seguridad en el móvil y redes sociales

El móvil es el dispositivo que más datos sensibles almacena. Protégelo con un PIN fuerte o biometría, mantén el sistema actualizado, revisa permisos de aplicaciones y descarga solo de tiendas oficiales. En redes sociales, usa contraseñas únicas, activa alertas de inicio de sesión, configura la privacidad y evita compartir información personal. Haz copias de seguridad periódicas de tus datos importantes.

Módulo 5 – Navegación segura en Internet

Muchos fraudes comienzan en páginas falsas. Revisa que la dirección tenga HTTPS y que el dominio sea correcto. Comprueba la reputación de las tiendas antes de comprar y usa métodos de pago seguros como tarjetas virtuales o PayPal. Evita conectarte a banca online en WiFi públicas; si es necesario, utiliza una VPN para proteger la conexión.

Módulo 6 – Protege tu dinero y tus datos

Accede siempre a la banca online desde la web oficial y activa 2FA para operaciones sensibles. Configura alertas de movimientos para detectar fraudes rápidamente. En compras online, utiliza tarjetas virtuales y plataformas seguras. Protege tus documentos y fotos en carpetas seguras y haz copias de seguridad en la nube o en discos externos. Evita publicar datos sensibles en redes sociales, pues pueden usarse para suplantar tu identidad.

Módulo 7 – Qué hacer si ya me hackearon

Si sospechas que fuiste hackeado, cambia inmediatamente tus contraseñas, activa 2FA y cierra sesiones abiertas. Usa los mecanismos de recuperación de cuentas de los servicios afectados. Si se filtraron datos bancarios, contacta con tu entidad y bloquea tarjetas. Denuncia el incidente y guarda evidencias como correos o capturas de pantalla. Después, refuerza tus cuentas y hábitos de seguridad para prevenir futuros ataques.

Módulo 8 – Cierre y plan personal

La seguridad digital depende de hábitos constantes. Como plan personal: cambia y gestiona contraseñas de forma segura, activa 2FA en todas tus cuentas importantes, desconfía de correos y enlaces sospechosos, revisa regularmente tus movimientos bancarios y realiza copias de seguridad de tus datos. Recuerda: la prevención es la mejor defensa y mantenerte atento reduce significativamente el riesgo de ser víctima de un fraude digital.