BUENAS PRÁCTICAS PARA PROTEGER TUS DISPOSITIVOS

Como docentes y colaboradores ITBA es necesario contar con buenas prácticas para la protección de los datos y la seguridad de los dispositivos.

Es fundamental tener conocimiento de los riesgos y amenazas que existen cuando navegamos, descargamos archivos de fuentes desconocidas y otro tipo de documentos que pueden poner en riesgo los equipos informáticos.

Se debe tomar conciencia que la seguridad comienza por un uso responsable de los dispositivos que utilizamos en el hogar o en la oficina.

Desde el área de Tecnologías de la Información te brindamos una serie de consejos y buenas prácticas para que puedas proteger tu equipo, resguardar tu información y protejas tus cuentas asociadas al Instituto Tecnológico de Buenos Aires.

Te recomendamos seguir con los siguientes consejos básicos para un uso responsable de tus dispositivos:

- Recordá crear contraseñas seguras en tus cuentas institucionales. Una contraseña segura puede ser creada con letras, números, símbolos, mayúsculas y minúsculas. Como mínimo 8 caracteres. También, recordá modificarla cada 30, 60 o 90 días.
- No compartas tus contraseñas con terceros. Recordá que con la contraseña de tu cuenta institucional podés acceder a todos los servicios ITBA, compartirla puede comprometer toda tu información personal y registro académico.
- Se recomienda **no utilizar la misma contraseña** en servicios externos a ITBA. Ya que si hay una filtración en algún servicio, el correo institucional y password pueden quedar expuestos a terceros.
- En el caso de utilizar redes sociales, servicios que no estén relacionados con ITBA o con el ámbito educativo/laboral se recomienda no utilizar la cuenta institucional para registrarse.

- Utiliza un doble factor de autenticación para brindar mayor protección en tus cuentas. Por ejemplo, para poder acceder a tu cuenta un requisito sería validarlo con tu teléfono móvil o con un SMS. Desde el siguiente link podés conocer los pasos para configurar el factor de doble autenticación en tu cuenta ITBA de Google: https://support.google.com/accounts/answer/185839?hl=es-419&co=GENIE.Platform%3DDesktop

- Realiza copias de seguridad (backups) de todos tus archivos regularmente de tus dispositivos para que en el caso de un incidente de seguridad cuentes con una copia de respaldo de tu información. Para ello podes usar Drive, espacio de almacenamiento proporcionado por el ITBA.

- No abras correos electrónicos sospechosos, este tipo de ataque se conoce como Phishing o ataques dirigidos de Spear Phishing. Generalmente puede llegar un correo electrónico donde se hacen pasar por un alumno, la institución o un servicio externo. ITBA y el Departamento de Tecnologías de la Información nunca te pedirá tu nombre de usuario y contraseña por correo electrónico para acceder a tu cuenta institucional o al SGA. Por ejemplo, un remitente podría hacerse pasar por el área de TI solicitandote información para actualizar la base de datos, esto incluye datos personales y otro tipo de datos sensibles. Este ataque se podría realizar también por Whatsapp u otro medio.

- No abras archivos sospechosos. Si te llega un archivo adjunto por correo electrónico que no solicitaste consulta con el remitente previamente antes de abrirlo porque podrías estar ejecutando un malware que podría comprometer la información de tu notebook o de la red ITBA. Por ejemplo, un remitente podría hacerse pasar por el área de Desarrollo Humano podría enviar un archivo adjunto por mail o por Whatsapp para que lo abras y ejecutes. Si el archivo contenía un código malicioso podrían acceder a tu equipo, robar información, espiarte, eliminar toda tu información o bloquear tu dispositivo.
  Ante cualquier duda comunícate con el área correspondiente para consultar sobre el pedido.

- Mantené actualizado tu antivirus, sistema operativo, navegador y software en tu PC. Si tenés mensajes de alerta de programas pendientes que necesiten actualización comunicate con ayuda@itba.edu.ar para que actualicen tu notebook. Si es la PC de tu hogar actualiza todo el software, ya que regularmente se actualizan problemas de seguridad en el software.

- Cuando navegas en la Web te recomendamos no descargar archivos que puedan ser sospechosos y puedan comprometer tu seguridad.

- Utiliza redes WiFi seguras. Evitá utilizar redes públicas o de aquellas que desconozcas su seguridad.

- Bloquea tu PC y dispositivos móviles cuando no lo estás utilizando. Por ejemplo, en tu celular utiliza una clave robusta para desbloquearlo y en la notebook cuando no la utilizas cerrá la sesión o configurá la opción de equipo desatendido.

- Si encontrás un pendrive, no lo utilices para ver el contenido ya que puede ser una memoria USB con código malicioso. Acércate a la Mesa de Ayuda y entrégalo ahí para que busquemos quien lo perdió.

- Ayuda TI no te va a pedir información personal sobre tu cuenta u otros datos personales por Whatsapp u otro medio de mensajería instantánea. No brindes información personal por este medio salvo que sean los canales oficiales de comunicación ITBA.

Para dudas, consultas o si querés reportar un incidente de seguridad podés hacerlo a ayuda@itba.edu.ar