

Checklist de Ciberseguridad Personal

Una guía práctica para proteger tus cuentas, contraseñas, dispositivos e información personal en internet.

Incluye	Para que sirve
Cuentas y contraseñas	Reducir el riesgo de accesos no autorizados.
Celular y computadora	Mantener tus dispositivos más seguros.
Redes Wi-Fi e internet	Evitar conexiones peligrosas y fraudes comunes.
Habitos digitales	Crear una rutina de seguridad fácil de mantener.

Este material es educativo. No reemplaza asesoría profesional de seguridad, pero te ayuda a mejorar tus hábitos digitales desde hoy.

1. Seguridad de cuentas

[] Usa contraseñas largas

Una contraseña segura debe tener 12 caracteres o mas. Mejor una frase larga que una palabra corta con símbolos.

[] No repitas contraseñas

Evita usar la misma contraseña en correo, redes sociales, banco o plataformas de estudio.

[] Activa verificación en dos pasos

Activa 2FA en correo, redes sociales, cuentas bancarias, almacenamiento en nube y plataformas importantes.

[] Cuida tu correo principal

Tu correo es la llave para recuperar muchas cuentas. Debe ser la cuenta mas protegida.

[] Revisa sesiones abiertas

Cierra sesiones en dispositivos que no reconozcas o que ya no uses.

2. Seguridad del celular y computadora

[] Actualiza el sistema

Las actualizaciones corrigen errores y vulnerabilidades. No las ignores por mucho tiempo.

[] Usa bloqueo de pantalla

Configura PIN, huella o reconocimiento facial. Evita códigos fáciles como 1234 o fechas obvias.

[] Instala apps solo de fuentes confiables

Descarga aplicaciones desde tiendas oficiales o sitios reconocidos.

[] Elimina apps que no uses

Menos apps significa menos riesgos y menos permisos innecesarios.

[] Haz copias de seguridad

Guarda información importante en una nube confiable o disco externo.

3. Internet, Wi-Fi y navegacion segura

[] Evita Wi-Fi publico para cuentas sensibles

No entres a bancos o cuentas importantes desde redes publicas sin proteccion.

[] Verifica enlaces antes de abrir

Desconfia de enlaces con errores, promociones exageradas o mensajes urgentes.

[] Revisa el candado HTTPS

El candado no garantiza que un sitio sea confiable, pero ayuda a confirmar que la conexion esta cifrada.

[] No descargues archivos sospechosos

Evita adjuntos o instaladores enviados por desconocidos.

[] Cuidado con premios y ofertas falsas

Si algo parece demasiado bueno para ser verdad, probablemente sea una trampa.

4. Proteccion contra phishing

El phishing es un intento de enganar a una persona para que entregue datos, contraseñas, códigos o dinero. Puede llegar por correo, SMS, WhatsApp, redes sociales o páginas falsas.

Senal de alerta	Que hacer
Mensaje urgente: "tu cuenta sera bloqueada"	No presiones enlaces. Entra manualmente al sitio oficial.
Errores de ortografia o dominios raros	Verifica el remitente y la direccion web.
Te piden codigos de verificacion	No compartas codigos 2FA con nadie.
Archivos inesperados	No abras adjuntos si no esperabas recibirlos.
Premios, regalos o descuentos extremos	Desconfia y busca informacion oficial.

5. Checklist semanal

- ☐ Cambiar contraseñas débiles o repetidas
- ☐ Revisar sesiones abiertas en correo y redes
- ☐ Actualizar celular y computadora
- ☐ Eliminar apps o extensiones que no uses
- ☐ Revisar permisos de aplicaciones
- ☐ Hacer copia de seguridad de archivos importantes
- ☐ Revisar movimientos o mensajes sospechosos

6. Reto practico ByteNova

Durante esta semana, elige 3 cuentas importantes y mejora su seguridad. Activa 2FA, cambia contraseñas repetidas y revisa si hay sesiones abiertas que no reconoces.

Mi avance:

Linea 1: _____

Linea 2: _____

Linea 3: _____

Linea 4: _____

ByteNova - Tecnologia explicada de forma clara, moderna y accesible.