DIGITAL SAFETY PLANNING

These 7 steps are designed to improve the digital health and safety of anyone at risk of being harmed online or via technology.

1 USE A SAFE DEVICE

What: If possible, safety plan from a safe device unknown to the attacker.

Concern: Safety planning steps could be exposed on a compromised device.

How: Use a device or computer belonging to a friend, the organization assisting you, etc.

2 CHANGE PASSWORDS

What: Update passwords to each account listed on the Accounts Checklist.

Concern: Compromised passwords can provide unauthorized access to accounts.

How: Use passwords the other party can't guess. Try a password manager to create and store passwords like LastPass or 1Password. Or use a phrase or sentence.

3 2-FACTOR AUTHENTICATION (2FA)

What: A 2nd layer of security in addition to your password. Sends a code to your phone or device that must also be entered to log in.

Concern: If not enabled, a person can log in with only the victim's password.

How: Enable 2FA on each account. If possible, set it up for every time you log in. Links to guides below:

Apple Google Facebook Instagram

4 REMOVE TRUSTED DEVICES

What: These are devices that accounts like Apple and Google recognize and trust.

Concern: Trusted devices won't require 2FA.

How: Log in to Apple or Google to view and remove any devices the victim doesn't trust.

5 LOG OUT OF ALL DEVICES

What: Attacker's device(s) may be still be logged in to victim's accounts.

Concern: Attacker can monitor or make changes to the victim's accounts.

How: Apple & Google allow you to log out all devices.

6 UPDATE CONTACT INFO

What: Email address & phone numbers where security notifications, 2FA codes & password reset links are sent.

Concern: Attacker may change a victim's contact info to a phone number or email they control.

How: Verify & update contact info for all accounts.

7 SECURITY QUESTIONS

What: Password reset questions & the attacker may know the answers.

Concern: The ability to reset a victim's password even after they change it.

How: Don't answer honestly. Change answers to something incorrect.

PLAN DE SEGURIDAD DIGITAL

Estos 7 pasos están diseñados para mejorar el bienestar y seguridad digital de cualquier persona en riesgo de ser maltratada por el internet o mediante la tecnología.

1 UTILISE UN APARATO SEGURO

Qué: Si es posible, cree su plan de seguridad desde un aparato seguro desconocido del agresor.

Preocupación: Los pasos de su plan de seguridad podrían quedar expuestos en un aparato comprometido.

Cómo: Use un aparato o computadora que pertenezca a un amigo, o la organización que le está ayudando, etc.

2 CAMBIAR CONTRSEÑAS

Qué: Actualice las contraseñas de cada cuenta que se encuentra en la Lista de verificación de cuentas.

Preocupación: Las contraseñas comprometidas pueden disponer acceso no autorizado a las cuentas.

Cómo: Use contraseñas que la otra persona no pueda adivinar. Pruebe con un administrador de contraseñas para crear y almacenar contraseñas como LastPass o 1Password. O usa una frase o oración.

3 AUTENTICACIÓN DE 2 FACTORES (2FA)

Qué: Una segunda capa de seguridad además de su contraseña. Esto envía un código a su teléfono o aparato que también se debe usar para entrar a una cuenta.

Preocupación: Si no se usa, una persona puede entrar a una cuenta con solamente la contraseña de la víctima.

Cómo: Active 2FA en cada cuenta. Si es posible, configúrelo cada vez que inicie sesión. Sitios de web a las guías a continuación:

Apple Google Facebook Instagram

4 ELIMINAR APARATOS DE CONFIANZA

Qué: Estos son los aparatos que las cuentas como Apple y Google reconocen y confían.

Preocupación: Los aparatos de confianza no requerirán 2FA.

Cómo: Inicie una sesión en Apple o Google para ver y eliminar cualquier aparato en la que la víctima no confíe.

5 CERRAR LAS SESIÓNES DE TODOS LOS APARATOS

Qué: Los dispositivos de los agresores todavía pueden estar conectados a las cuentas de la víctima.

Preocupación: El agresor puede monitorear o hacer cambios en las cuentas de la víctima.

Cómo: Apple & Google se permiten cerrar sesión en todos los aparatos.

6 ACTUALIZAR LA INFORMACIÓN DE CONTACTO

Qué: El correo electrónico y los números de teléfono donde se envían notificaciones de seguridad, códigos 2FA y enlaces de restablecimiento de las contraseñsa.

Preocupación: El atacante puede cambiar la información de contacto de la víctima a un número de teléfono o correo electrónico que controle.

Cómo: Verifique y actualice la información del contacto de todas las cuentas.

7 PREGUNTAS DE SEGURIDAD

Qué: Preguntas de restablecimiento de contraseña, el atacante podría saber las respuestas.

Preocupación: La capacidad de restablecer lacontraseña de una víctima incluso después de quela cambien.

Cómo: No des una respuesta verdadera. Cambie las respuestas a algo incorrecto.