****

Computación Básica:
Mantenerte seguro en línea

Lesson Plan

**Objetivos:**

Al final de la clase, el estudiante podrá:

* Crear una contraseña fuerte con una combinación de letras y números.
* Identificar y evitar daño a causa de emails de *phishing*, cupones y ofertas de trabajo fraudulentas.
* Identificar y evitar mensajes pop-up.
* Evaluar sitios web para determinar su seguridad y confiabilidad.

**Antes de la clase**

* Cargar la presentación de Powerpoint: Mantenerte Seguro\_slides.ppt
* Inscríbete en una cuenta de email y de Facebook

**Resumen de la clase**

90 minutos

1. **¿Porque necesitamos contraseñas?**
	1. Como cerradura para tus cuentos en línea.
	2. Discusión: ¿Qué tipos de sitios las piden?
		1. Email
		2. Negocios- comprar cosas en línea
		3. Bancos
		4. Bills/cuentas
		5. Redes sociales
		6. Aplicaciones de trabajo
2. **Cómo hacer una buena contraseña**
	1. Mantener equilibrio entre fuerte y fácil de recordar
		1. **Discusión:** ¿Cómo podemos crear contraseñas memorables pero difíciles de adivinar?
			1. Evitar nombres de hijos y esposos.
			2. Basarlas en cosas favoritas – bandas, películas o actores.
			3. Basarlas en la letra de un poema o una canción favorita.
	2. PPT diapositiva: Características
		1. 8 caracteres
		2. Substituye letras por números
		3. Mezcla de letras, números y símbolos
		4. Sin información personal
		5. Pista: comida, música, equipo o frase favorita
	3. PPT diapositiva: sustituyendo números por letras
	4. **Ejercicio: Crear contraseñas**
		1. Abre el internet, ve a google.com y busca “comprueba password”
			1. Haz clic en el primer resultado, http://www.internautas.org/compruebapassword.html
		2. **Demostración** (con Vicente Fernández, El Elvis de México):
			1. Teclea “vicente” (débil).
			2. Teclea “Vicente” (mejor).
			3. Teclea “Vicente!” (mejor).
			4. Teclea “V1c3nt3!” (muy fuerte!).
		3. **Actividad**: cada estudiante tiene que crear una contraseña que reciba un 70% o más.
3. **Cambiando tus contraseñas en las cuentas que ya tienes**
	1. Busca “settings” (a veces se parece a un engrane (una rueda con dientes))
		1. Demuestra cómo se hace en gmail
			1. Haz clic en “hola tu nombre”-> Mi Cuenta ->Cambia tu contraseña
		2. Demuestra cómo se hace en Facebook
			1. Haz clic en el engrane (rueda con dientes) Configuración de la cuenta -> contraseña -> Editar…. -> guardar cambios
	2. **Discusión:** ¿Es una buena idea usar la misma contraseña para todos los sitios? ¿Por qué sí o por qué no?
4. **Cuidado con email**
	1. ¿Qué es phishing? (la pesca de tu identidad por personas que quieren suplantar su identidad)
	2. Ver video de commoncraft en español http://www.commoncraft.com/video/phishing-scams
	3. **Cómo reconocer email de phishing**
		1. Sin nombre
		2. Van a pedir información personal
		3. Amenazas
		4. Errores
		5. Parecen venir de una organización legítima
	4. PPT diapositivas: Ver ejemplos 1 y 2
		1. Pedir que un estudiante los lea en voz alta
		2. **Discusión**: ¿Por qué es sospechoso?
			* Sin nombre
			* Piden información personal
			* Amenazas
			* Errores
			* Parecen venir de una organización legítima
	5. **¿Qué debes hacer si recibes un email de phishing?**
		1. No hagas clic
		2. Bórralo
			1. Mostrarles cómo borrar un email de *phishing* en su cuenta de email abierta.
		3. No respondas
5. **Cuidado con las búsquedas de trabajo**
	1. PPT diapositiva: Ver EmpleoPhishing.
	2. Oferta de empleos fraudulenta
	3. Similar a *phishing* (errores, sin nombre, sospechoso, piden información)
	4. Hay muchas ofertas fraudulentas en craigslist.com, pero también muchas buenas oportunidades
6. **Otras estafas en línea**
	1. **Gangas** (deals y coupons)
		1. Es demasiado bueno para ser la verdad.
		2. Van a ofrecerte cosas gratuitas como computadoras, iPhones o certificados de regalo.
		3. Quieren tu información personal.
		4. Muchas veces, estas estafas de ganga aparecen en **Pop-ups.**
			1. PPT: mirar los pop-ups
	2. **Pop-ups**
		1. ¿Qué es un pop-up? Un anuncio o mensaje de la computadora que se abre en una nueva ventana sin ninguna acción de tu parte
			1. Algunos son normales o necesarios, y otros son malos.
		2. **Normales**- **un mensaje para ti de la computadora.**
			1. Léelo- ¿qué tienes que hacer? Por lo general, harás clic en ok.
			2. PPT: mira ejemplos de pop-ups “normales”
		3. **Mal** – ***fingen* ser un mensaje de la computadora.**
			1. Quieren robar tu información o instalar una virus.
			2. PPT: mira ejemplos de “pop-ups malos”
				* ¿Cómo puedes reconocerlos?
			3. ¿Qué tienes que hacer? -
				* Alt F4- ¡no oprimas nada!
		4. **Cuidado con las redes sociales**
			1. Estados en Facebook que fingen ser gangas, pero no lo son.
7. **Confiabilidad de Internet**
	1. Repasar dominios con la clase
	2. PPT slide- las tres preguntas
	3. Abrir google.com y buscar “formulario migración eeuu”
		1. El primer resultado es un negocio. Lee “acerca de nosotros”
		2. Regresa a la página de resultados y busca algo con el dominio .gov
	4. PPT diapositiva: HTTP v HTTPS
		1. Demostrarles que la cuenta de email abierta tiene una https.