

Victor Eduardo Morales Bernal

Presidente de la Comisión de Ciberseguridad de la ABM

Director de Seguridad de la Información en Banco Azteca

#BANCAEXPLICA

15 años de experiencia en la banca

21 años de experiencia en **Ciberseguridad**



Victor Eduardo Morales Bernal

Presidente de la Comisión de Ciberseguridad de la ABM

Director de Seguridad de la Información en Banco Azteca

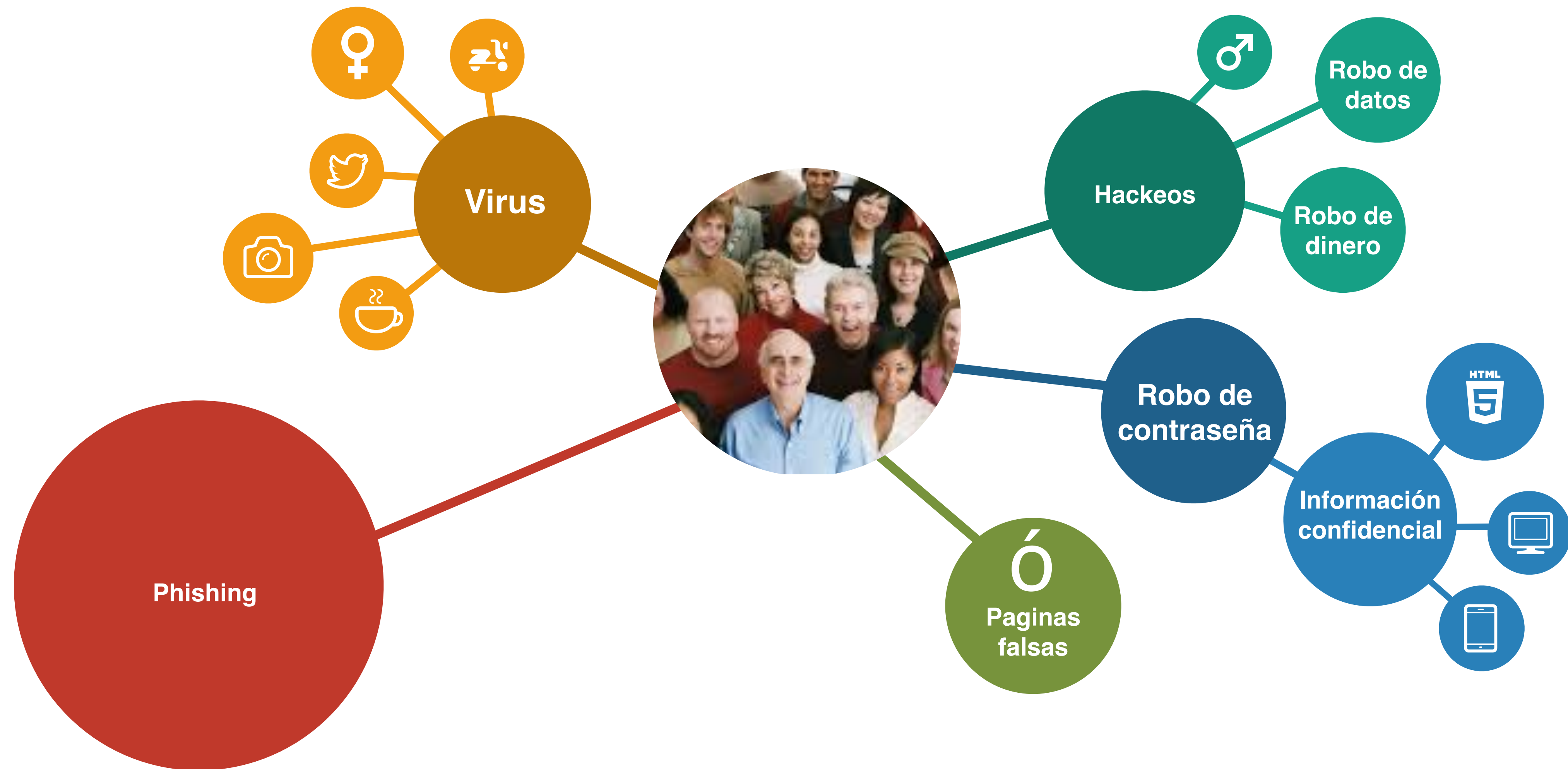
#BANCAEXPLICA

Protégete, que no te engañen: la ciberseguridad la hacemos todos



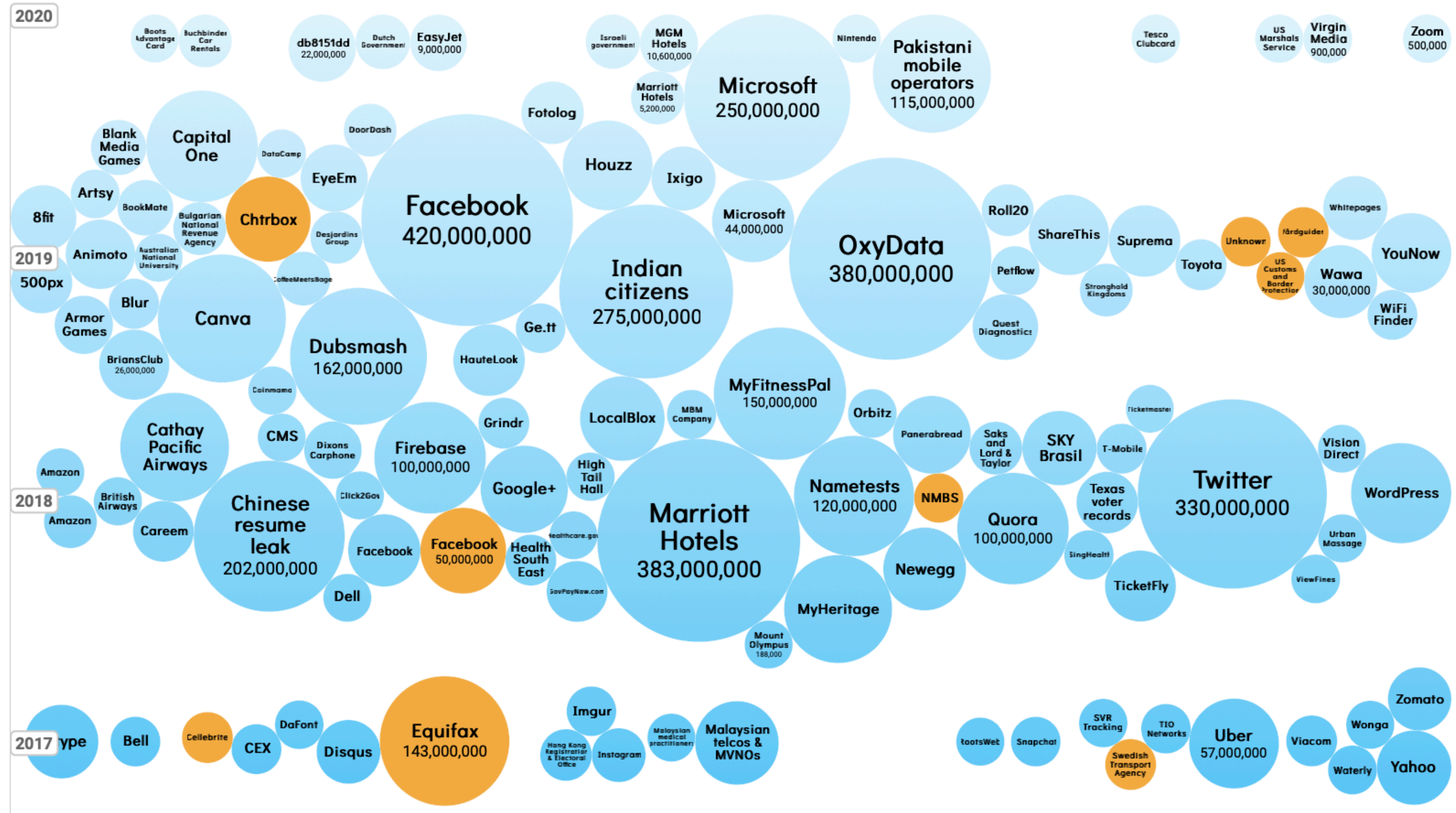
Riesgos permanentes

Usuarios en general



Riesgos permanentes

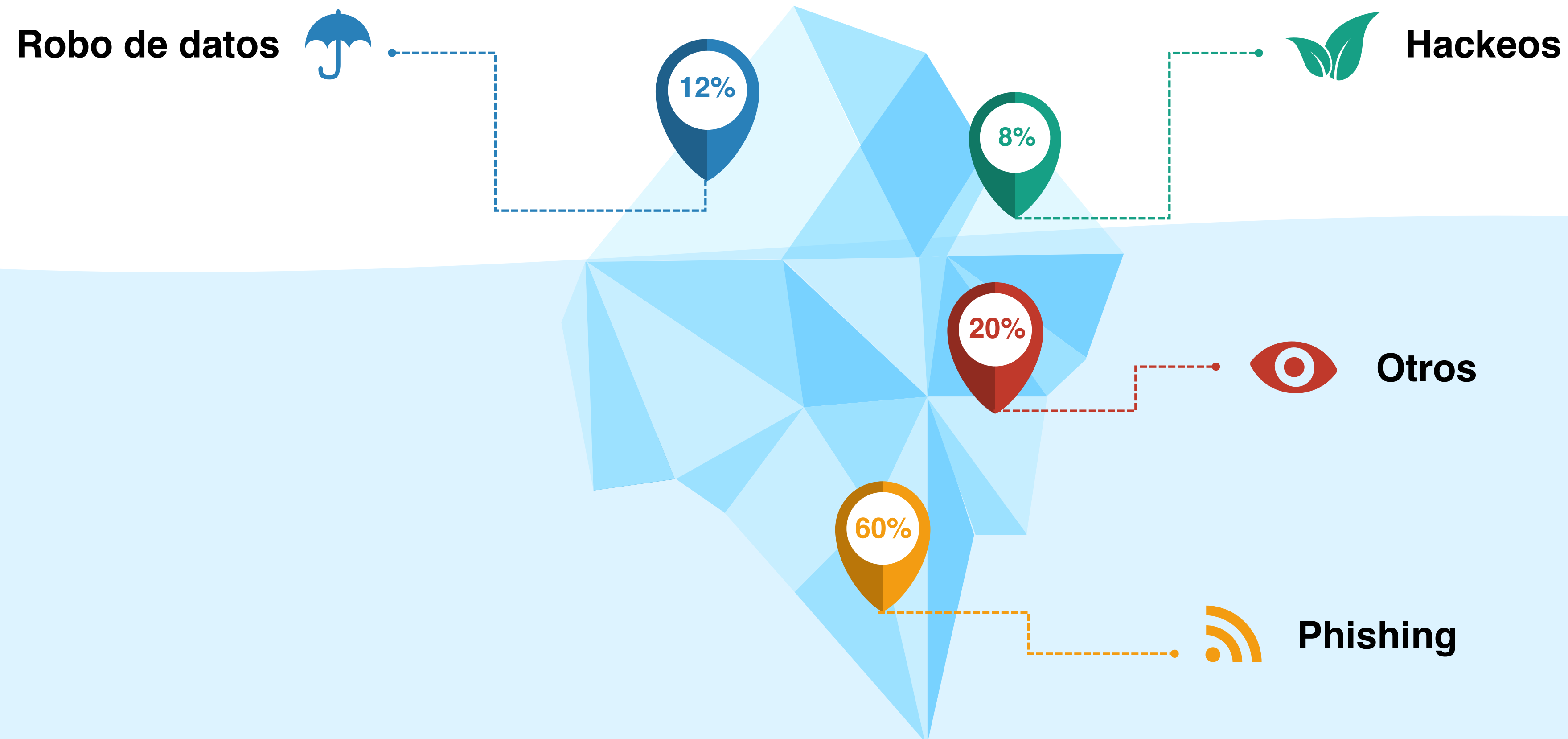
Algunos ataques en el mundo



Fuente: Information is beautiful - data breaches

Riesgos permanentes

Usuarios en general





Phishing

¿Qué es?

Phishing es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.

Algunos tipos de phishing

Lo más común



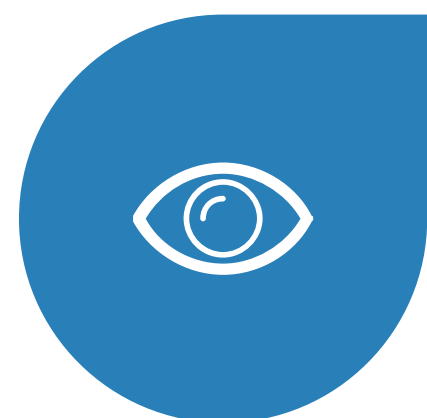
¿A quién va dirigido?

Lo más común





¿Por qué?



Datos

Cuentan con algunos datos que nos hacen pensar que lo que estamos viendo o escuchando es verdad



Engaños

Mediante técnicas de ingeniería social a través de engaños, obtienen información que permita robarnos datos o bienes económicos



Cultura

Se aprovechan de una falta aún de cultura de cuidado de la información y en ocasiones, se enfocan en diferentes brechas generacionales

Algunos ejemplos

Fraudes

Una supuesta cadena de supermercados muy famosa nos llama por teléfono y **nos ofrece un premio de regalo para gastar en sus tiendas**. Una vez que nos mostramos interesados, el atacante tratará de hacer que compartamos todos nuestros datos personales y/o datos de la tarjeta de crédito, con la excusa de que son necesarios para esta promoción. En ocasiones, tratará de invitarnos a acceder a una web fraudulenta, compartir la promoción con otros usuarios a través de nuestras redes sociales o aplicaciones de mensajería instantánea, rellenar un formulario con nuestros datos personales, etc.

No es normal que de la nada ganemos un premio y que a parte nos pidan datos personales de nuestra tarjeta. ¡Que no te engañen!

Algunos ejemplos

Fraudes

Un supuesto técnico de un banco se pone en contacto con nosotros por teléfono para **informarnos de una incidencia que podría afectar gravemente al sistema de nuestra computadora**. Para solucionarla lo antes posible, están llevando a cabo controles en remoto en los equipos de aquellos usuarios afectados. Dejándolo en manos del experto, terminamos por confiar en él, descargamos el **software** que necesita y le **damos control sobre nuestro equipo** para que acceda a nuestros archivos, robe nuestros datos o instale *software* malicioso.

Tu banco nunca te pedirá datos sensibles ni mucho menos te ofrecerá soporte remoto a tus dispositivos o equipos de computo. ¡Que no te engañen!

Algunos ejemplos

Fraudes

A hand holding a black smartphone with a blank screen. The phone is held vertically, and the hand is visible on the left side of the frame. The background is a solid grey color.

Nuestro teléfono comienza a sonar y una chica muy amable nos informa de que aún estamos a tiempo **de participar en un sorteo o promoción inexistente a través de alguna red social de un supuesto banco**. Parece que se trata de una promoción de una conocida marca que busca recompensar a sus clientes. Tras describir el premio, nos pide que compartamos una serie de datos por temas legales, como nuestro nombre, apellidos, correo, dirección así como hábitos de consumo sobre nosotros y nuestra familia. Recopilados nuestros datos, no volveremos a tener noticias sobre el sorteo.

Tu banco nunca te pedirá datos sensibles ni te hará ganar un premio que nunca te informo. Si tienes duda, acércate a tu banco. ¡Que no te engañen!

¿Cómo nos protegemos?



Información personal

Nunca proporcionar información personal y confidencial como contraseñas, token, CVVs, otros



Números desconocidos

Duda siempre de números desconocidos y cualquier aclaración, acércate primero a tu banco



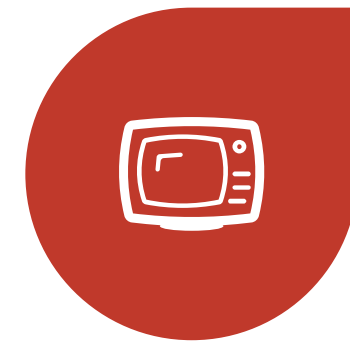
Sitios oficiales

Nunca visites o descargues aplicaciones que no sean sitios autorizados por tu institución



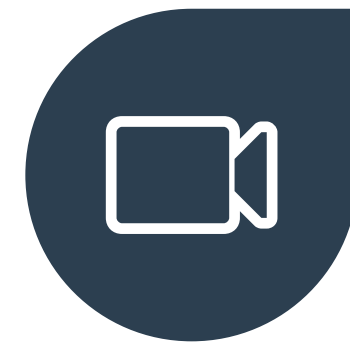
SMSs

Si recibes un SMS de un supuesto cargo a tu tarjeta y te piden marcar a un número que no ubicas, acércate a tu banco primero y nunca contestes los mensajes de este tipo



Correos

No hagas caso a correos que no provengan de un remitente autorizado por tu banco y mucho menos des clic a ligas que podrían llevarte a sitios fraudulentos



Virus

Manten instalado siempre un antivirus actualizado en tus dispositivos

Protégete, que no te engañen: la ciberseguridad la hacemos todos

¿Cómo nos protegemos?

Protégete, que no te engañen



**No respondas
a ningún SMS con tus
datos personales**

ABM ASOCIACIÓN
DE BANCOS
DE MÉXICO

CONDUSEF
COMISIÓN NACIONAL PARA LA PROTECCIÓN
Y DEFENSA DE LOS USUARIOS DE
SERVICIOS FINANCIEROS

¿Cómo nos protegemos?

Protégete, que no te engañen

Spoofting

El defraudador disfraza su número telefónico para que aparezca el nombre de tu banco en el identificador y así solicitar tus datos confidenciales.



¿Cómo nos protegemos?

Protégete, que no te engañen

Smishing

A través de un mensaje de texto (SMS), el defraudador simula ser tu banco o una empresa, para ganar tu confianza y pedir tu información confidencial.



ABM ASOCIACIÓN DE BANCOS DE MÉXICO

CONDUSEF

¿Cómo nos protegemos?



Protégete, que no te engañen

**Tu banco conoce
tus datos
personales, no te
llama para
pedírtelos.**

ABM ASOCIACIÓN
DE BANCOS
DE MÉXICO

CONDUSEF
COMISIÓN NACIONAL PARA LA PROTECCIÓN
Y DEFENSA DE LOS USUARIOS DE
SERVICIOS FINANCIEROS

Victor Eduardo Morales Bernal

Presidente de la Comisión de Ciberseguridad de la ABM

Director de Seguridad de la Información en Banco Azteca

#BANCAEXPLICA

Protégete, que no te engañen: la ciberseguridad la hacemos todos

