XIX Jornada de Actualización Bancaria - 2021

El Phishing Bancario: efectos y responsabilidades del sector financiero

18 de noviembre de 2021

AGENDA

- **Definición**
- **Riesgos**
- **Circuito de un ataque**
- **Algunos Datos Estadísticos**
- **Efectos en la banca**
- **Responsabilidades de la Banca**
- **¿Cómo prevenirlo? (Clientes y Colaboradores)**
- **Ejemplos de Banderas Rojas**

GLOBAL BANK
Primero la gente

Definición

- **Phishing**
- **Ingeniería Social**

GLOBAL BANK
Primero la gente

¿QUE TIPO DE INFORMACIÓN ROBAN?

Datos personales
Direcciones de Correo
No. Documento de Identidad
Datos de localización y contacto

Información financiera
No. de tarjetas de crédito
Números de cuentas
Información de Home Banking o E-commerce

Credenciales de acceso
Redes sociales
Cuentas de correo

PRINCIPALES MEDIOSDE PROPAGACIÓN

- Correo eléctronico
- Redes Sociales
- SMS/MMS
- Llamados telefónicos
- Infección de Malware

¿Cuáles son los riesgos de un ataque de Phishing?

La amenaza de la ingeniería social y el phishing es un problema significativo en todos los países y organizaciones cuyos principales riesgos son:

- **Suplantación de Identidad**
- **Robo de Dinero**
- **Utilización de cuentas para actividades delictivas**
- **Fraude**
- **Venta de datos personales**

CIRCUITO DE UN ATAQUE

Algunos datos estadísticos

¿Cuántos ataques de phishing fueron dirigidos a su empresa? (Datos de 2019)

75% de las organizaciones alrededor del mundo experimentaron algún tipo de ataque de phishing en 2020.

GLOBAL BANK
Primero la gente

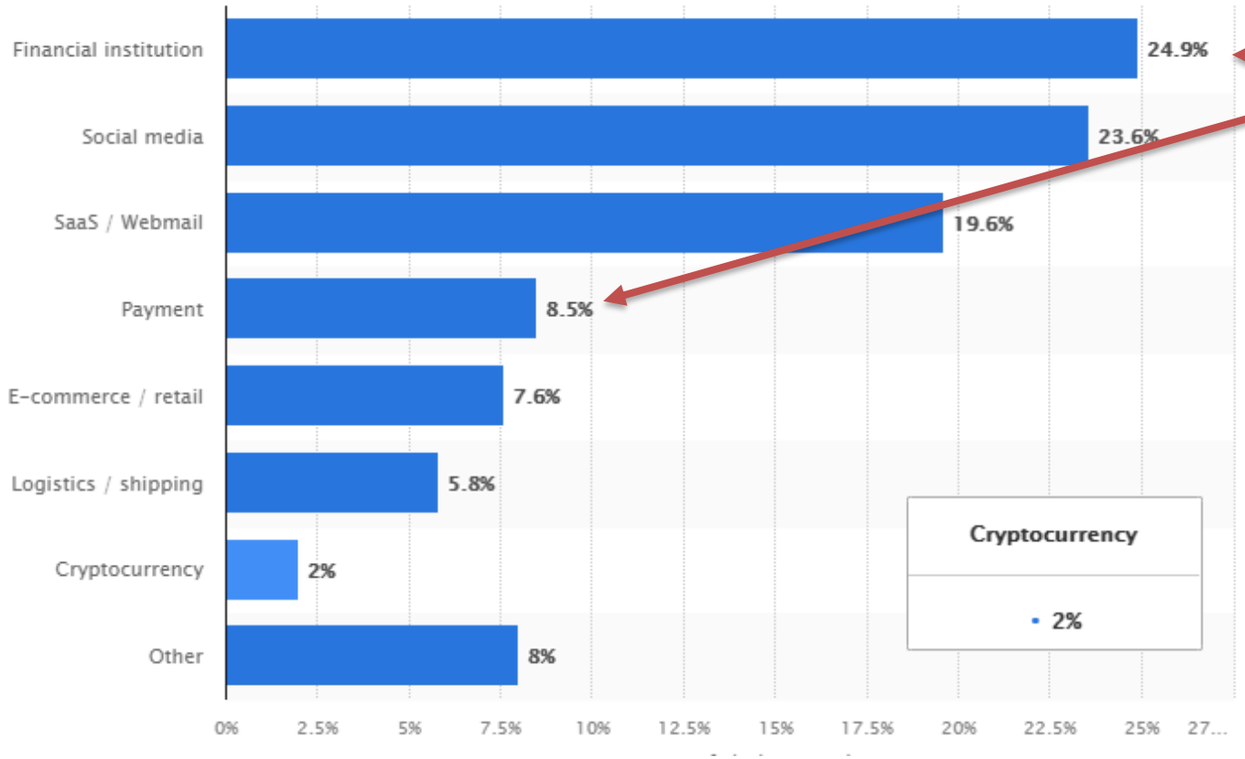
96% de los ataques de Phishing llegan por correo electrónico.

Costo promedio de registro comprometido: $150
Costo promedio de brecha de datos: $3.92 millones

Consecuencias de los ataques de Phishing (según líderes de seguridad alrededor del mundo.

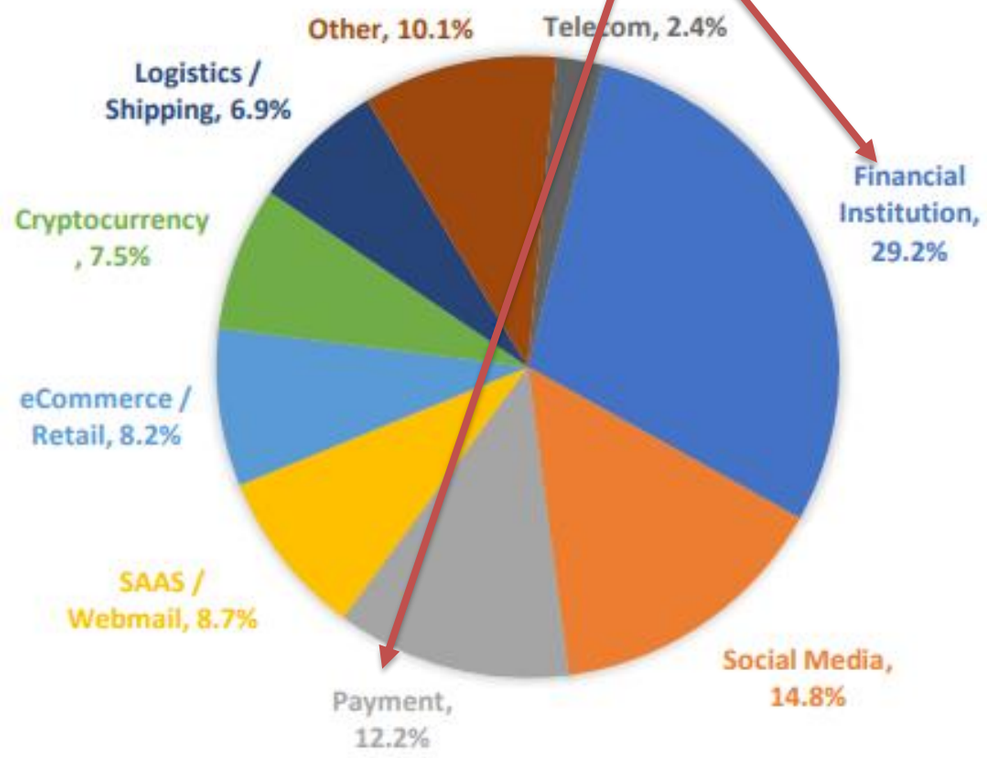
- 60% de las organizaciones perdieron data.
- 52% de las organizaciones tuvieron credenciales de cuentas comprometidas.
- 47% de las organizaciones fueron infectadas con ransomware.
- 29% de las organizaciones fueron infectadas con ransomware.
- 18% de las organizaciones experimentaron pérdidas financieras.

GLOBAL BANK
Primero la gente



1Q2021 – 24.9% Instituciones Financieras + 8.5% en Pagos

2Q2021 – 29.2% Instituciones Financieras + 12.2% en Pagos



Q1 a Q2 - 2021

+4.3% en Instituciones Financieras

+3.7% en Pagos

Google Safe Browsing

- Sitios web de phishing subieron 27% entre ene-2020 y ene-2021 (de 1.69 millones a 2.145 millones).
- En el mismo periodo, sitios de malware subieron de 21,803 a 28,802 (32%).

ESET (Q3-2020)

Adjuntos maliciosos más comunes:

1. Ejecutables de Windows (74%)
2. Scripts (11%)
3. Documentos de Office (5%)
4. Archivos Comprimidos (4%)
5. Otros (6%)

Asuntos más comunes en correos de Phishing - 4Q2020

1. IT: Annual Asset Inventory
2. Changes to your health benefits
3. Twitter: Security alert: new or unusual Twitter login
4. Amazon: Action Required | Your Amazon Prime Membership has been declined
5. Zoom: Scheduled Meeting Error

¿Cuánto podría llegar a ganar un atacante?

Sólo 0.5% hace click

20% de los que hacen click ingresa datos bancarios

$10 por cuenta (ejemplo)

GLOBAL BANK
Primero la gente

¿Por qué las Instituciones Financieras somos el blanco #1?

- Se estima que el sector bancario en Latinoamérica crezca un **10% en 2022**
- Por la pandemia, mayor enfoque en **Digitalización** y **Trabajo Remoto**
- Usabilidad y Diseño vs. Infraestructura y Arquitectura de Seguridad
- Rapidez en Adopción Digital vs. Foco en Seguridad
- Falta de familiaridad de los clientes en técnicas de Phishing
- 90% de los ciberataques en Latinoamérica Latina concentrados en Brasil, México y Colombia. Ningún país de la región está en los 20 primeros de ciberataques de alto impacto entre 2006 y 2020

GLOBAL BANK
Primero la gente

Efectos en la Banca

A Nivel Individual

- Pérdida de Datos Personales
- Pérdida de Credenciales
- Pérdida de Dinero
- Suplantación de Identidad
- Víctima de Ransomware

A Nivel Corporativo

- Daño a la reputación de la marca
- Problemas legales
- Multas
- Pérdida de información confidencial de colaboradores y clientes
- Pérdida significativa de ingresos
- Pérdida de propiedad intelectual
- Vandalismo en línea
- Horas de Trabajo perdidas
- Costos de Remediación y Respuesta

GLOBAL BANK
Primero la gente

Responsabilidades de la Banca

- Usar el principio del “Buen Padre” con los clientes para apoyarlos en educación y prevención de este tipo de ataques.

- Trabajar en tres pilares: Políticas, Tecnología y Educación

GLOBAL BANK
Primero la gente

¿**Cómo prevenirlo**? (Clientes y Colaboradores)

- Verifique los remitentes y sus dominios de email. Si el mensaje parece urgente o alarmante, contactar al banco o al remitente por otra vía.
- Digite siempre la dirección web en la barra indicada de su navegador y revisar los URLs que te envían pasando el mouse por encima.
- Asegúrese de que la dirección del sitio web comience con HTTPS.
- Mantenga su navegador de internet y el sistema operativo de su dispositivo actualizados.
- Verifique con regularidad sus estados financieros.
- Recuerde utilizar contraseñas que no se relacionen con usted y cámbielas con frecuencia. Utilice Autenticación de doble factor o biométrica para proteger tus cuentas.
- No acceda a ninguna cuenta financiera ni personal mediante una red pública y cierre la sesion al terminar.

Banderas Rojas

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

Verificar dirección del remitente, puede que no sea legítimo.

From: MasterCard <reembolsos@mastercard_latam.com.pa>
Reply-to: MasterCard <reembolsos@mastercard_latam.com.pa>
Subject: Has recibido una devolución de pago

Hola lisbethb@globalbank.com.pa

Hemos enviado un pago de $ 595.22 a su cuenta de comerciante el 28 de mayo 2021. Puede encontrar los detalles de este pago a continuación.

Total Settlement Amount.....$595.22

Location	Amount Paid
XXXXXX5191	$595.22

Tenga en cuenta que pueden pasar algunos días hasta que esta información se refleje en su cuenta bancaria.

Para ver todos sus estados de pago, haga clic aquí. También puede visitarnos en mastercard-payments.com/merchant para actualizar o administrar su cuenta de comerciante.

Mover el mouse sobre cualquier enlace, que aparezca en el cuerpo del correo. Antes de hacer clic, verificar que la dirección sea correcta.

Ver Cuenta Bancaria

Suplantación de Identidad de la empresa. Evita Caer en las trampas!

Regards,
Mastercard Merchant Care

THE RED FLAGS OF ROGUE URLs

Spotting malicious URLs is a bit of an art. The examples represented here are some of the common tricks used by hackers and phishers to fool users into visiting malicious websites. The methods shown here could be used by legitimate services, but if you see one of these "tricks" you need to make sure you're dealing with the organization you think you are.

Look-a-Alike Domains

Domain names which **seem** to belong to respected, trusted brands.

Slight Misspellings

Microsoftnline
<v5pz@onmicrosoft.com>

www.llnkedin.com

Brand name in URL, but not real brand domain

ee.microsoft.co.login-update-dec20.info

www.paypal.com.bank/logon?user=johnsmith@gmail.com

ww17.googlechromeupdates.com/

Brand name in email address but doesn't match brand domain

Bank of America
<BankofAmerica@customerloyalty.accounts.com>

Brand name is in URL but not part of the domain name

devopsnw.com/login.microsoftonline.com?userid=johnsmith

URL Domain Name Encoding

https://%77%77%77.%6B%6E%6F%77%62%654.%63%6F%6D

Shortened URLs

When clicking on a **shortened URL**, watch out for malicious redirection.

https://bit.ly/2SnA7Fnm

Domain Mismatches

Human Services .gov
<Despina.Orrantia6731610@gmx.com>

https://www.le-blog-qui-assure.com/

Strange Originating Domains

MAERSK
<info@onlinealxex.com.pl>

Overly Long URLs

URLs with 100 or more characters in order to **obscure the true domain**.

http://innocent website.com/irs.gov/logon/fasdjkg-sajdkjnd fjnbkasldjfbkajsdbfkjbasdf/adsnfjksdngkfdfgfgjhfgd/ght.php

File Attachment is an Image/Link

It looks like a file attachment, but is really an **image file with a malicious URL**.

PDF INV39391.pdf
52 KB

https://d.pr/free/f/jsaeoc
Click or tap to follow link.

Open Redirectors

URLs which have hidden links to completely different web sites at the end.

t-info.mail.**adobe.com**/r/?id=hc347a&p1=**evilwebsite.com**

01DSSB34R01

KnowBe4
Human error. Conquered.