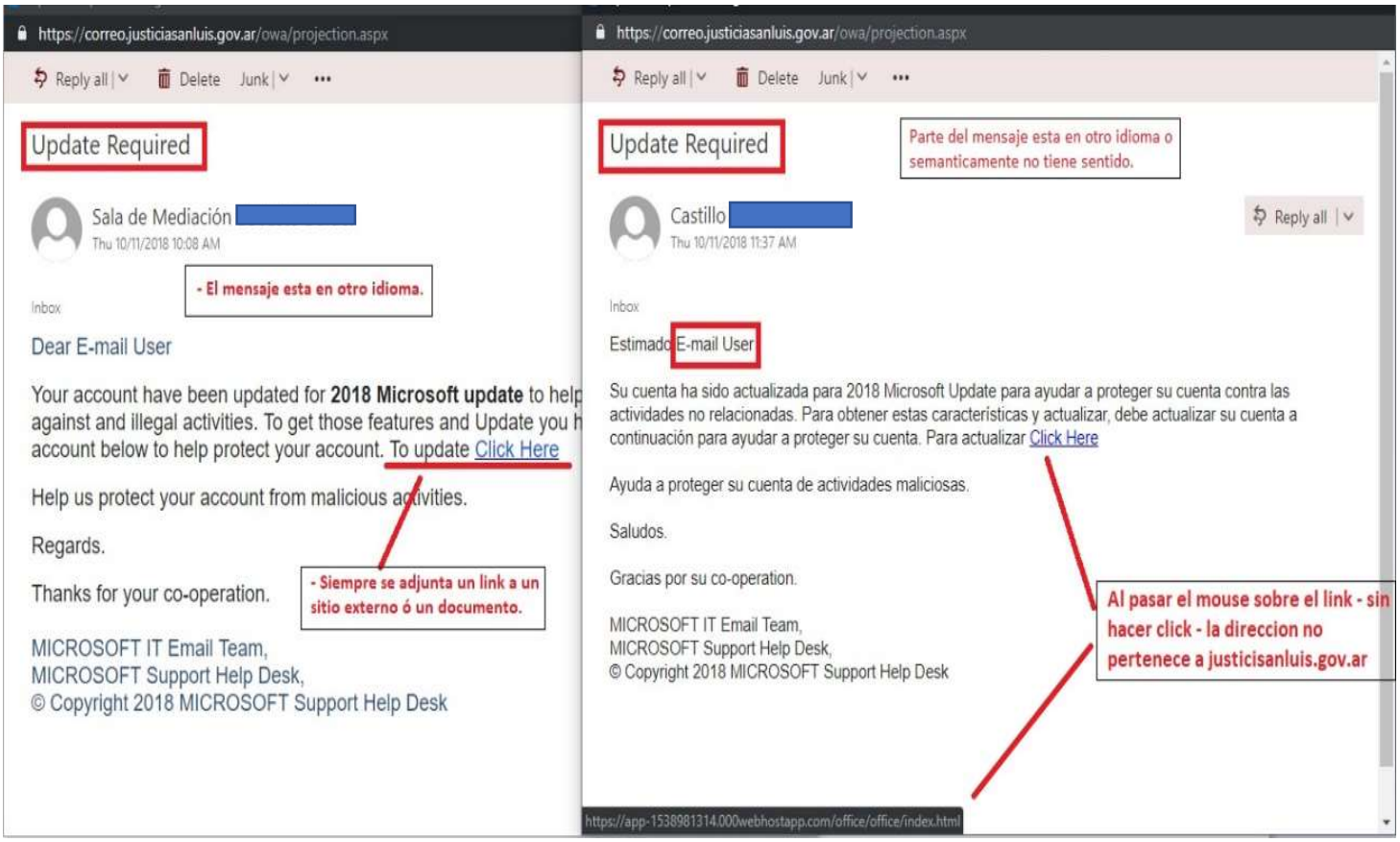
¿Qué es el phishing?

El Phishing o fraude informático, tiene como objetivo engañar al usuario para obtener información confidencial de este, la cual será utilizada posteriormente para suplantar su identidad digital o robar información personal (claves de acceso).

A pesar de la implementación de sistemas anti SPAM y la actualización constante de los mismos, no hay en el mundo sistema 100% seguro o infranqueable. Esta pequeña guía pretende dar algunos consejos a la hora de identificar correos fraudulentos.

¿El contenido es sospechoso? ¿La escritura es correcta?

Para identificar un phishing lo primero es valorar el contenido del mensaje, los delincuentes suelen intentar hacerse pasar por: el soporte técnico, administrador de correo, un banco, una plataforma de pago, una red social, un servicio público, etc.



¿Pide hacer algo de manera urgente? ¿Quién envía el correo?

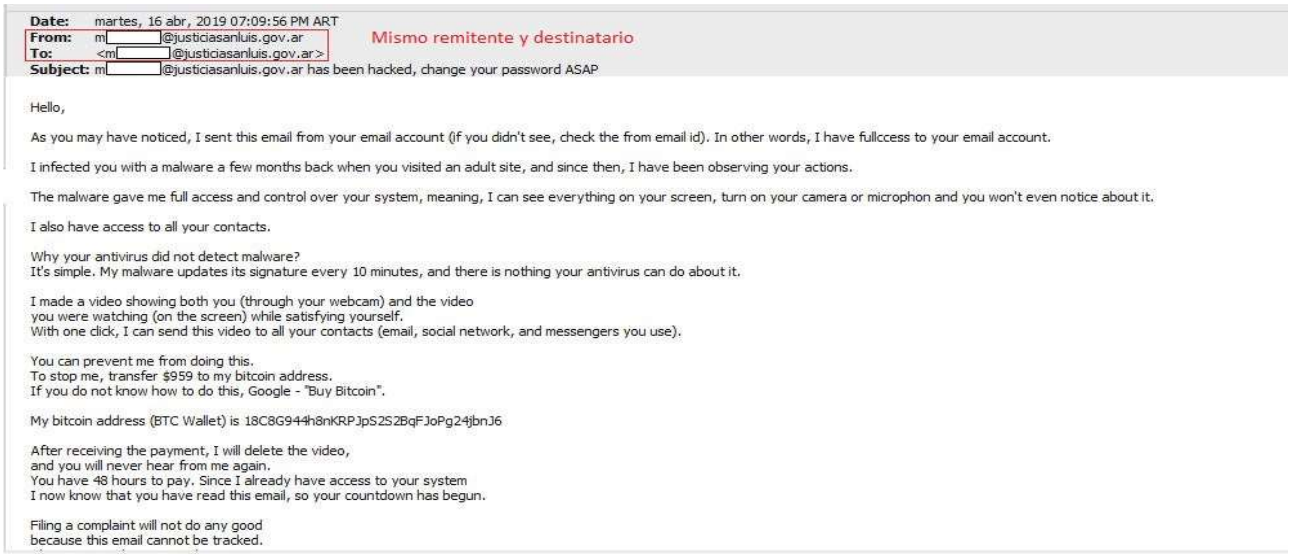
Con frecuencia se pide tomar acciones de forma inmediata. Esta supuesta "urgencia" es utilizada por los delincuentes para intentar que su víctima tome una decisión precipitada y caiga en el engaño, que incluye visitar un enlace a un sitio fraudulento e indicar datos personales y/o contraseñas.

Como se puede observar el remitente que aduce ser un "**ADMIN**istrador", envía el correo desde otro dominio diferente al "**@justiciasanluis.gov.ar**".

En otras ocasiones el atacante puede infectar un dispositivo (celular, PC, notebook, etc.) donde el usuario tiene configurada su cuenta de correo y generar correos automáticos con el objeto de simular correos genuinos para tratar de engañar a otros contactos del usuario infectado. Algunas de las características recurrentes para estos tipos de correos son:

- Suelen dirigirse de forma genérica para evitar decir un nombre, ej.: Estimado cliente", "Hola", "Hola amigo", etc.
- Suele venir textos en otros idiomas y con errores de ortografía, y se usan herramientas dedicadas que generan contenido de forma automática.

- Se suele agregar links o enlaces a otros sitios, con el objeto de que el usuario realice alguna acción de mantenimiento o que introduzca datos sensibles, *ej: solicitar que el usuario actualice su contraseña en sitios maliciosos que simulan ser sitios genuinos.*



Date: martes, 16 abr, 2019 07:09:56 PM ART
From: m[redacted]@justiciasanluis.gov.ar
To: <m[redacted]@justiciasanluis.gov.ar>
Mismo remitente y destinatario
Subject: m[redacted]@justiciasanluis.gov.ar has been hacked, change your password ASAP

Hello,

As you may have noticed, I sent this email from your email account (if you didn't see, check the from email id). In other words, I have fullccess to your email account.

I infected you with a malware a few months back when you visited an adult site, and since then, I have been observing your actions.

The malware gave me full access and control over your system, meaning, I can see everything on your screen, turn on your camera or microphon and you won't even notice about it.

I also have access to all your contacts.

Why your antivirus did not detect malware?
It's simple. My malware updates its signature every 10 minutes, and there is nothing your antivirus can do about it.

I made a video showing both you (through your webcam) and the video
you were watching (on the screen) while satisfying yourself.
With one click, I can send this video to all your contacts (email, social network, and messengers you use).

You can prevent me from doing this.
To stop me, transfer $959 to my bitcoin address.
If you do not know how to do this, Google - "Buy Bitcoin".

My bitcoin address (BTC Wallet) is 18C8G944h8nKRPJpS2S2BqFJoPg24jbnJ6

After receiving the payment, I will delete the video,
and you will never hear from me again.
You have 48 hours to pay. Since I already have access to your system
I now know that you have read this email, so your countdown has begun.

Filing a complaint will not do any good
because this email cannot be tracked.

Como recomendación final, ante cualquier duda relacionada a

"CORREO NO DESEADO O PHISHING"

les recordamos que pueden acercarse por cualquiera de nuestras oficinas o

directamente realizar la consulta vía correo a:

informaticasl@justiciasanluis.gov.ar (Informática San Luis)
informaticavm@justiciasanluis.gov.ar (Informática Villa Mercedes)
informaticacon@justiciasanluis.gov.ar (Informática Concarán)
informaticamf@justiciasanluis.gov.ar (Informática Multifuero)