CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ciber diccionario

1.- AUTENTICACIÓN DE DOBLE FACTOR (2FA):

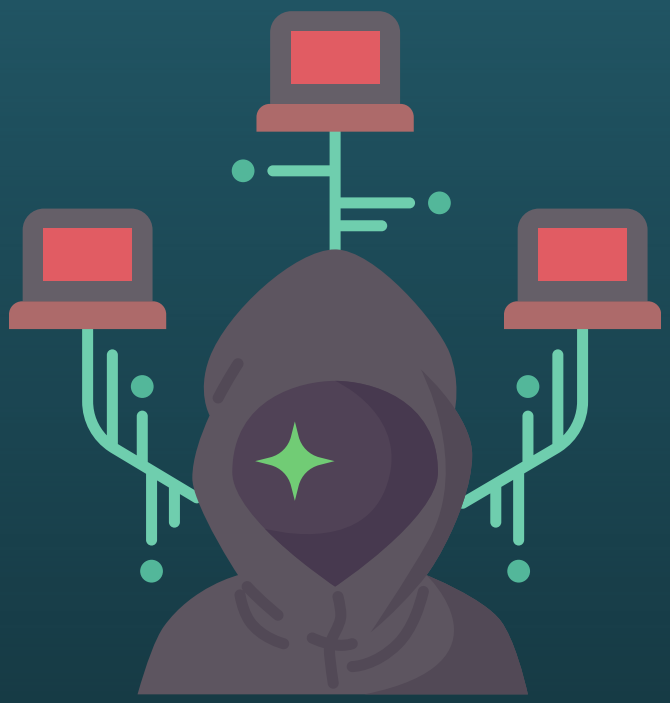
Procedimiento que permite comprobar que un usuario es quien dice ser al ingresar a un equipo o aplicación, realizando esta verificación en dos pasos. Primero, con una contraseña y luego con otros datos que pida el sitio, mediante un método distinto al usado en la primera autenticación. Esto, con el objetivo de contar con equipos y programas más protegidos.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ciber diccionario

2.- BOTNET:

Esta palabra se formó a partir de los términos en inglés “robot” y “network” y se refiere a un conjunto de computadores (denominados bots) controlados de forma remota por un atacante, sin que los usuarios sepan lo que ocurre en sus equipos, con la finalidad de llevar a cabo distintas acciones maliciosas.



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ciber diccionario

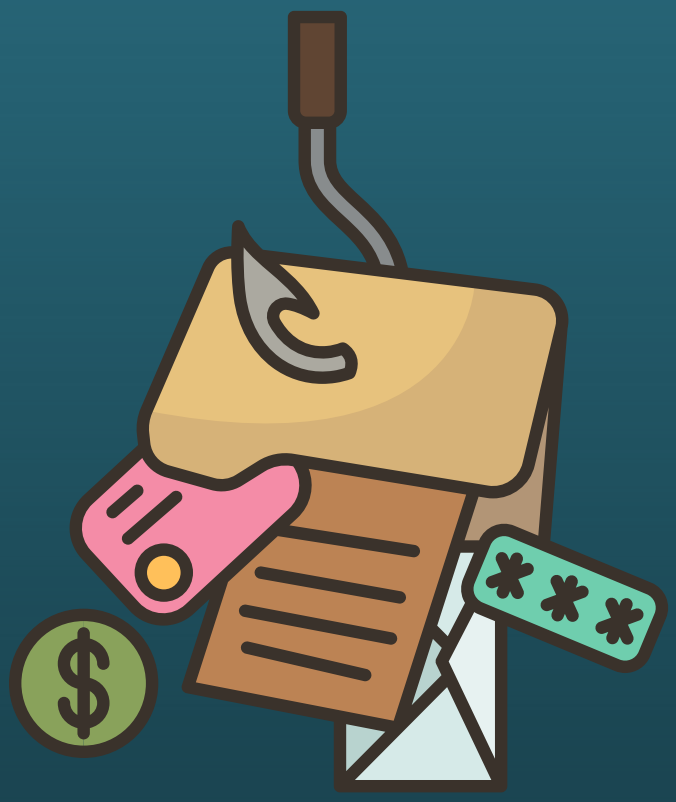
3.- INGENIERÍA SOCIAL:

Técnica que utilizan los ciberdelincuentes para manipular a las personas, ganarse su confianza y así obtener su información personal para acceder, por ejemplo, de forma ilegítima a sus cuentas bancarias. Para lograr su cometido, los atacantes utilizan campañas de phishing.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ciber diccionario

4.- PHISHING:



Engaño que se realiza mediante un correo electrónico u otra forma de comunicación, como SMS y apps de mensajería. Los delincuentes invitan a las personas a ingresar a un enlace adjunto en el correo o bajar un archivo, para redirigir a una página web falsa y así robar información personal o para descargar un programa malicioso (o malware) en el equipo.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ciber diccionario

5.- SPAM:

También conocido como correo no deseado, se refiere a los mail recibidos con remitente desconocido o información no solicitada, y que son enviados de forma masiva.