ES

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

De enero de 2019 a abril de 2020

Phishing

Panorama de Amenazas de la ENISA

Sinopsis

El *phishing* es el intento fraudulento de robar datos de usuarios, como las credenciales de apertura de sesión, datos de tarjetas de crédito o incluso dinero, utilizando técnicas de ingeniería social. **Este tipo de ataque suele efectuarse a través de mensajes de correo electrónico, que parecen proceder de un remitente seguro y que tienen la intención de persuadir al usuario para que abra un documento adjunto malintencionado o pinche en un enlace a una URL fraudulenta**. Existe una forma de *phishing* dirigida a un objetivo muy específico (*spear phishing*) que cuenta con información previa sobre las víctimas para que la estafa parezca más auténtica y que hace que sea uno de los tipos de ataque de más éxito en redes de empresas.[1]

La respuesta emocional justifica muchas de las acciones de las personas cuando son víctima de un ataque de *phishing* y eso es exactamente lo que buscan los ciberdelincuentes. En un contexto de formación, ese efecto debe ser el objetivo de una simulación de *phishing*. Enseñar a los usuarios de correo electrónico es una de las medidas de prevención del *phishing* que suelen utilizarse, pero los resultados no son convincentes, ya que los delincuentes cambian constantemente su *modus operandi*. La conformidad con el estándar DMARC (autenticación de mensajes, informes y conformidad basada en dominios) garantiza el bloqueo de mensajes procedentes de dominios fraudulentos, lo que reduce las probabilidades de éxito de los ataques de *phishing*, *spoofing* y correo basura[2].

A corto plazo el correo electrónico seguirá siendo el mecanismo principal de *phishing*, pero no a largo plazo. Ya se está viendo un aumento en el uso de mensajes de redes sociales, WhatsApp y similares, para realizar ataques. El cambio más relevante se producirá en los métodos utilizados para enviar los mensajes, que se harán más sofisticados con la adopción, por parte del adversario, de métodos de inteligencia artificial para preparar y enviar mensajes. *Phishing* y *spear phishing* son vectores de ataque importantes de otras amenazas como las amenazas internas involuntarias[2].

Conclusiones

26 200_ millones de pérdidas en 2019 por ataques BEC (compromiso de los mensajes de correo electrónico de la empresa).[20]

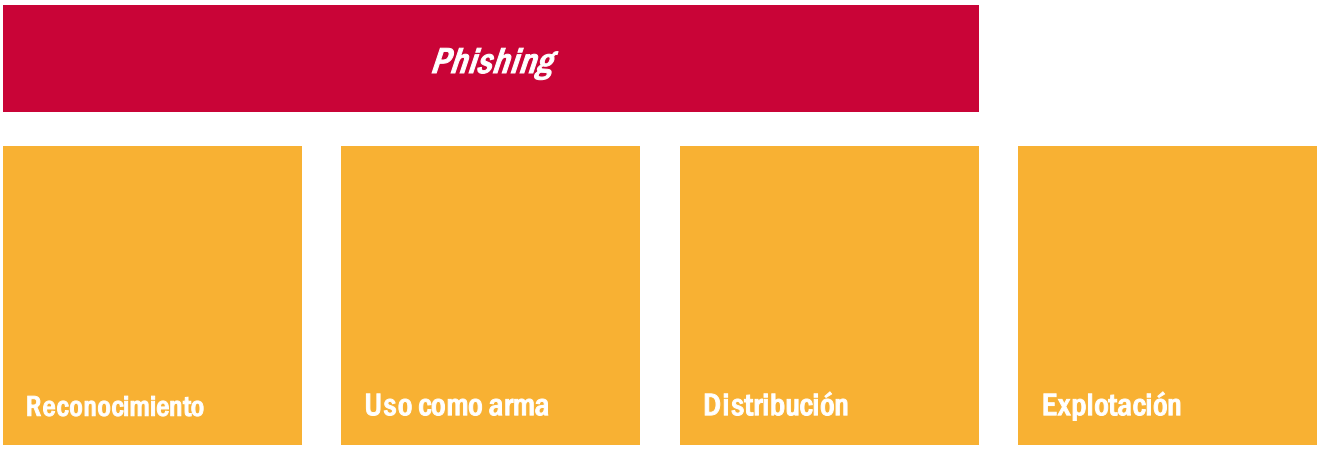
42,8 %_ de los adjuntos malintencionados fueron documentos de Microsoft.[25]

667 %_ de aumento en estafas de *phishing* en tan solo 1 mes durante la pandemia de COVID-19.[6]

30 %_ de los mensajes de *phishing* se distribuían los lunes.[29]

32,5 %_ de todos los mensajes enviados usaban la palabra «pago» en la línea de asunto del mensaje.[28]

Kill chain



Paso del proceso de ataque

Amplitud de la intención

Lockheed Martin desarrolló el marco cibernético de Kill Chain® que adaptó a partir de un concepto militar relacionado con la estructura de un ataque. Para estudiar un vector de ataque determinado, utilice este diagrama de *kill-chain* para trazar cada paso del proceso y anotar las herramientas, técnicas y procedimientos utilizados por el atacante.

MÁS INFORMACIÓN

Tendencias

_Los tipos de servicios más atacados son los de correo *web* y los de software como servicio

Según indican algunas proyecciones, los ataques de *phishing* dirigidos a los servicios de *software* como servicio (software-as-a-service, SaaS) y *webmail* superaron a los dirigidos a los servicios de pago por primera vez en el primer trimestre de 2019; lo que los convierte en el sector más afectado (36 %) por los ataques de *phishing*.[2] Este nuevo récord sigue la tendencia de 2018 en la que los servicios SaaS y de *webmail* acababan de adelantar al sector financiero[3]. Aunque la cifra había bajado a un 30,8 % a finales de 2019, los servicios mencionados anteriormente siguen siendo los primeros de la lista[2,3]; con **los servicios de Microsoft 365 como objetivo principal de los *phishers***.[4]

_Los ataques BEC siguieron siendo un problema

En un estudio reciente se identificó que el 88 % de las organizaciones de todo el mundo había sufrido ataques de *spear phishing* y que un 86 % de ellas había sufrido ataques BEC.[16] En 2019, uno de los servicios más atacados fue el de Microsoft 365 y el foco se centró en recabar credenciales.[17] Una vez conseguidas estas credenciales, el atacante podía recabar más datos de la organización, un proceso que podía durar semanas o meses[18] y que podía llevar a ataques de *spear-phishing*. El atacante simula ser un empleado, el director ejecutivo o incluso un proveedor de confianza para desviar fondos o redirigir pagos a cuentas de terceros.[14] En el primer trimestre de 2019, las empresas fueron víctimas de ataques BEC con un 120 % más de frecuencia que el año anterior[19], lo que resultó en pérdidas que ascendían a los 26 200 millones de dólares estadounidenses (aprox. 22 200 millones EUR).[20]

Más de dos tercios de los sitios de *phishing* adoptaron HTTPS

En los últimos años se ha producido un aumento pronunciado[13] en el número de sitios de *phishing* que han adoptado HTTPS. En el último trimestre de 2019, un 74 % de los sitios de *phishing* utilizaron HTTPS[32], un aumento importante en comparación con el 32 % de tan solo 2 años atrás. Aunque las tecnologías como la HTTPS y la SSL se han diseñado para proteger las comunicaciones entre el cliente y el servidor, la presencia de un icono de candado en la barra de direcciones del navegador puede crear la falsa ilusión de que el sitio *web* es seguro.

Los atacantes también podrían utilizar sitios legítimos que han pirateado para albergar contenido de *phishing* y que hacen que sea difícil para el usuario final identificar el sitio como inseguro[14]. Otros factores que contribuyen a este aumento pronunciado en el uso de HTTPS son la gran cantidad de servicios de certificación gratuitos, como Let's Encrypt[15] y el hecho de que los navegadores actuales marcan todos los sitios HTTPS como seguros, sin comprobaciones adicionales.

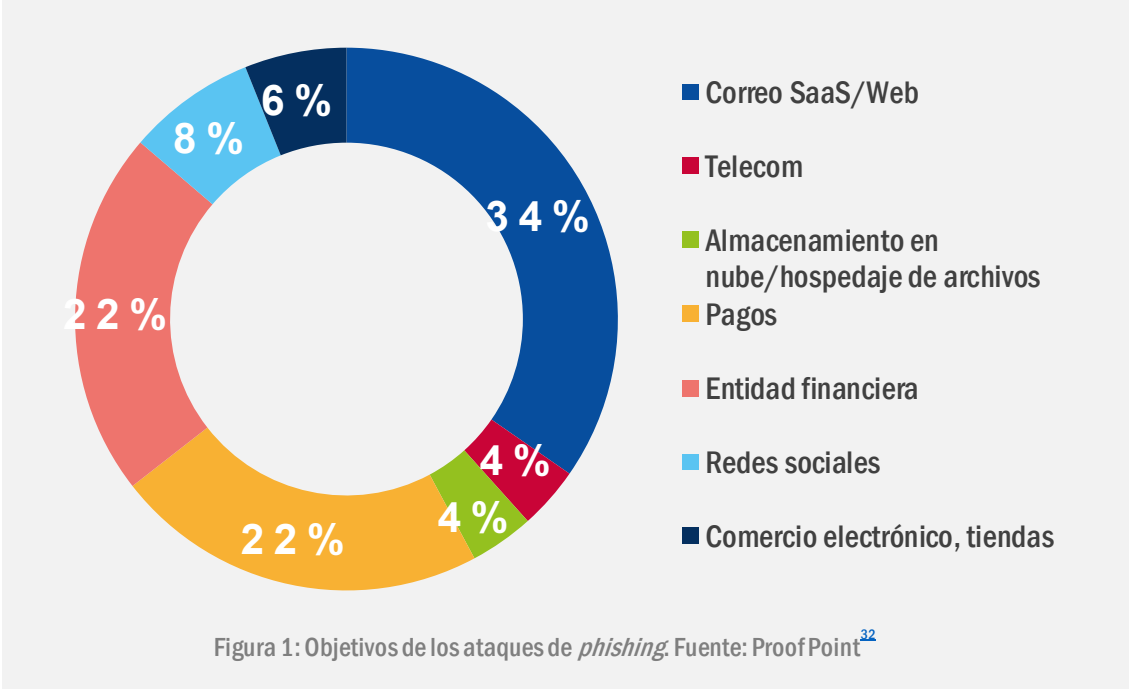


Figura 1: Objetivos de los ataques de *phishing*. Fuente: Proof Point[32]

Tendencias

_Aumento del *phishing* como servicio (PhaaS)

Estos tipos de servicios suelen estar disponibles por suscripción o en forma de *kit*, que se puede descargar previo pago, y que permiten eliminar las barreras tecnológicas para adoptar este tipo de ataques, ya que pueden utilizarlos personas con menos capacidades técnicas. En un informe de un investigador especializado en temas de seguridad[21] se identificaron 5 334 *kits* de *phishing* distintos disponibles en junio de 2019. Lo que es todavía más preocupante es el bajo coste de estas soluciones: una suscripción mensual cuesta entre 50 y 80 dólares estadounidenses. En el mismo informe se revelaba que el 87 % de los *kits* incluían mecanismos de evasión, como la codificación de caracteres HTML y el cifrado de contenido. Es interesante destacar que algunos de estos servicios se alojaban en servicios en la nube legítimos con nombres y certificados DNS (sistema de nombres de dominios) correctos. Las estadísticas de uno de estos puntos de venta en la *dark net* indican el elevado grado de éxito de estos ataques, que permiten al atacante individual o grupo de atacantes robar alrededor de 65 000 cuentas al mes.[22]

_Tendencias de los incidentes

- Se ha producido un cambio en la eficacia de los ataques de *phishing* que usan el almacenamiento en nube, DocuSign y servicios en la nube de Microsoft.
- Para que las campañas de *phishing* sean más eficaces, los ataques de impostores incluyen engaños como el de compromiso de los mensajes de empresa (BEC) y técnicas de simulación de identidades basadas en ingeniería social.
- El *phishing* dirigido a los servicios de Microsoft 365 fue el engaño principal, pero el foco sigue estando centrado en la recolección de credenciales.
- Más del 99 % de los mensajes de correo electrónico malintencionados requerían intervención humana (pinchar enlaces, abrir documentos, aceptar avisos de seguridad y otros similares) para ser eficaces.[44]

Temas principales de *phishing* en 2019

- Recolección genérica de credenciales por correo electrónico
- *Phishing* en cuentas de Office 365
- *Phishing* en instituciones financieras
- *Phishing* en Microsoft OWA
- *Phishing* en OneDrive
- *Phishing* en American Express
- *Phishing* en Chalbhai Generic
- *Phishing* en cuentas Adobe
- *Phishing* en Docusign
- *Phishing* en Netflix
- *Phishing* en cuentas Dropbox
- *Phishing* en cuentas LinkedIn
- *Phishing* en cuentas Apple
- *Phishing* en empresas de correos y transporte
- *Phishing* en Microsoft Online Document (Excel y Word)
- *Phishing* en la configuración de Windows
- *Phishing* en Google Drive
- *Phishing* en PayPal

Fuente: Proof Point[32]

Tendencias

_La pandemia de COVID-19 utilizada como anzuelo de *phishing*

Los ciberdelincuentes se están aprovechando del miedo del público por la pandemia de COVID-19, que se inició a finales de 2019. Se ha informado de que los ataques de *phishing* relacionados con el virus aumentaron un 667 % en un período de 1 mes (desde finales de febrero de 2020 a finales de marzo de 2020), y que estos tipos de engaños representaron de por sí un 2 % de todos los delitos de *phishing*.[5]

En estos engaños se enviaban mensajes de *phishing* diseñados para parecer que el remitente era el Centro de Control de Enfermedades (CDC) de Estados Unidos[6], la Organización Mundial de la Salud[7] o, incluso, equipos de investigación de universidades[8]. En ellos se informaba falsamente de los casos de infección en el área de la víctima o compartían las opiniones de expertos médicos para que la víctima mordiera el anzuelo y pinchara en el enlace malintencionado. Esto ha hecho que el FBI y la OMS hayan emitido notificaciones de aviso.[8,9] Dado que durante la cuarentena muchas personas trabajaban desde casa, en muchos casos utilizando sistemas de seguridad no actualizados[11], los ciberdelincuentes intentaban explotar oportunidades y vulnerabilidades[12].

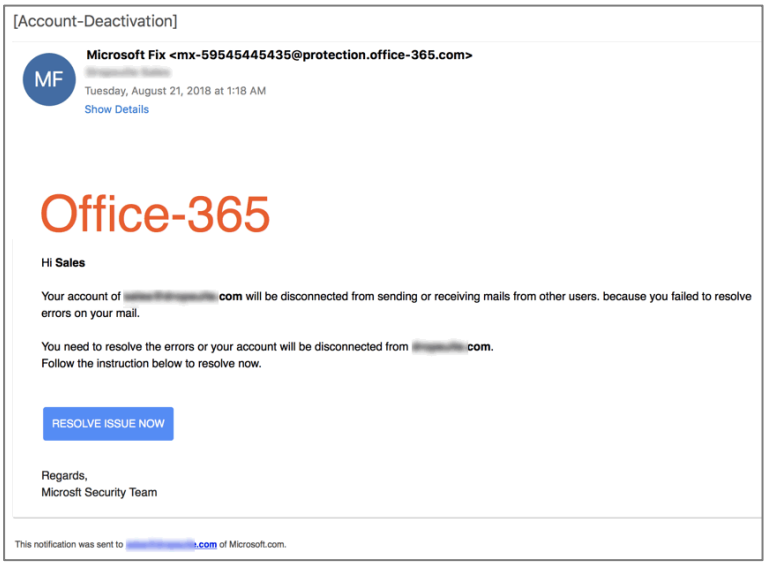


Figura 2: Mensaje de *phishing* en Office 365. Fuente Dropsuite[45]

La respuesta de la ENISA a la pandemia de COVID-19

La pandemia de COVID-19 ha hecho que cambiemos nuestra forma de vivir. En este mundo cada vez más conectado, tenemos la suerte de poder seguir trabajando o viviendo nuestras vidas privadas de forma virtual. Durante este momento sin precedentes, la Agencia Europea para la Ciberseguridad (ENISA) compartió sus recomendaciones en materia de ciberseguridad[46] sobre una serie de temas, que incluían el teletrabajo, las compras por Internet y los servicios sanitarios electrónicos; también proporcionó actualizaciones sobre el asesoramiento en temas clave relacionados con la seguridad adaptados a los sectores afectados. La ENISA revisa el panorama de amenazas durante la pandemia y produce asesoramiento sobre cómo mitigar los riesgos que presentan las amenazas más críticas. Se ha prestado una especial atención al tema del *phishing* debido al aumento en el número de ataques.

Figura 3: Vídeo de YouTube de la ENISA sobre la COVID-19. Fuente: ENISA

Incidentes

Los sectores más atacados

El sector de la sanidad fue el más afectado por los ataques de *phishing* (o de *spear-phishing*) en 2019. Un investigador especializado en temas de seguridad[42] llegó a la conclusión de que el *phishing* fue el vector de ataque principal de este año, mediante el uso de tácticas de ingeniería social para distribuir mensajes infectados con *malware* o con enlaces que llevaban a sitios *web* infectados. Otros sectores que también sufrieron ataques fueron las entidades gubernamentales y otras entidades de las administraciones públicas. Por ejemplo, en noviembre y diciembre de 2019, varios diplomáticos y funcionarios del gobierno de Ucrania recibieron mensajes de *spear-phishing* que los dirigían a sitios *web* peligrosos.[43]

Vectores de ataque

La técnica del *spear-phishing* sigue siendo una forma de acceso inicial muy frecuente utilizada por los atacantes. Estos agentes utilizan una serie de tácticas de ingeniería social para inducir a los destinatarios de los mensajes a abrir documentos adjuntos o visitar un sitio *web* infectado. Los mensajes de *spear-phishing* suelen contener documentos de Microsoft Office que contienen macros malintencionadas o un enlace a estos documentos. Cuando un usuario selecciona la opción «Habilitar el contenido», la macro interna empezará la ejecución de una serie de *scripts* ocultos que resultan en la descarga de la primera fase de *malware*. JavaScript y PowerShell parecen ser los lenguajes de programación más habituales para esta actividad.

Ejemplos

_Un ataque de *phishing* dirigido contra los estudiantes de la Universidad de Lancaster dio como resultado la pérdida de datos personales.[37]

_Los ciberdelincuentes realizaron ataques de *phishing* para obtener credenciales de apertura de sesiones de 2 500 usuarios de Discord.[38]

_Un proveedor de servicios de salud física fue víctima de un ataque de *phishing*.[39]

_Pacientes afectados por el ataque de *phishing* a UConn Health.[41]

_Una subsidiaria del sector de la automoción perdió 37 millones de dólares estadounidenses (aprox. 31 millones EUR) en un engaño BEC.[33]

Mitigación:

_Acciones propuestas

- Enseñar al personal a identificar mensajes falsos y malintencionados y a estar alerta. Lanzar campañas de *phishing* simuladas para probar la infraestructura de la organización y la respuesta del personal.
- Considerar el uso de una pasarela de correo electrónico con un mantenimiento periódico (posiblemente automatizado) de los filtros (filtros *antispam*, *antimalware* y basados en políticas).
- Considerar la aplicación de soluciones de seguridad que utilizan el aprendizaje automático para identificar sitios de *phishing* en tiempo real.
- Desactivar la ejecución automática de código, macros, procesamiento de gráficos y de precarga enviados por correo en los clientes de correo y actualizarlos frecuentemente.
- Implementar uno de los estándares de reducción de mensajes de correo basura: SPF (Marco de directivas de remitente)[34], DMARC (Autenticación de mensajes, informes y conformidad basada en dominios)[35] y DKIM (Correo con Identificación por DomainKeys).[36]
- Lo ideal es utilizar comunicaciones seguras por correo electrónico con firmas digitales o encriptado, para las transacciones financieras vitales o cuando se intercambia información sensible.
- Implementar detección de fraude y anomalías a nivel de red para los mensajes entrantes y salientes.
- Evitar pinchar en enlaces aleatorios, especialmente en los enlaces abreviados que se presentan en las redes sociales.
- No pinchar en los enlaces o adjuntos descargados si no se tiene total certeza de la procedencia del mensaje.

- Evitar compartir demasiada información personal en las redes sociales; p. ej., duración del tiempo que se va a estar fuera de la oficina, información de vuelos, etc., ya que es información que los atacantes utilizan activamente para recabar información sobre sus objetivos.
- Comprobar el nombre de dominio de los sitios *web* que se visitan para ver si tiene errores de escritura, especialmente sitios *web* sensibles, como los bancarios. Los atacantes normalmente registran dominios falsos que tienen un aspecto similar a los verdaderos y los usan para «pescar» a sus objetivos. No es suficiente con ver si la conexión es HTTPS.
- Activar la autenticación de dos factores siempre que sea posible para evitar secuestros de cuentas.
- Utilizar una contraseña robusta y única para cada servicio en línea. Reutilizar la misma contraseña para varios servicios es un problema de seguridad importante y debe evitarse en todo momento. Usar credenciales robustas y únicas para cada servicio en línea limita el riesgo de un posible secuestro de cuenta a solo el servicio afectado. Utilizar software de gestión de contraseñas ayuda a gestionar todas las contraseñas.
- Cuando se envía dinero a una cuenta es importante comprobar la información de la cuenta destinataria a través de otro medio. No se debe confiar en los mensajes de correo electrónico sin encriptar y sin firmar, especialmente en casos sensibles.
- Comprobar cómo funcionan los formularios de contacto, registro, suscripción y comentarios en su sitio *web* y añadir reglas de verificación si fuera necesario a fin de que los atacantes no puedan explotarlos.

Bibliografía

1. "What Is Phishing?". Cisco. https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

2. "Phishing Activity Trends Report Q1". 2019. APWG. https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf

3. "2018 Phishing Trends & Intelligence Report" 2018. Phishlabs.

https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report_2018-digital.pdf

4. "Microsoft remains phishers' #1 target for the fifth straight quarter". 22 de agosto de 2019. Vade Secure.
https://www.vadesecure.com/en/phishers-favorites-q2-2019/

5. "Threat Spotlight: Coronavirus-Related Phishing". 26 de marzo de 2020.
https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/

6. "Coronavirus phishing emails: How to protect against COVID-19 scams" 2020. https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html

7. "Covid-19 Drug Advice From The WHO Spoofed to Distribute Agent Tesla Info-Stealer". 2020. IBM.
https://exchange.xforce.ibmcloud.com/collection/Covid-19-Drug-Advice-From-The-WHO-Disguised-As-HawkEye-Info-Stealer-2f9a23ad901ad94a8668731932ab5826

8. "Abnormal Attack Stories #6: Coronavirus Credential Theft". 13 de marzo de 2020.
https://abnormalsecurity.com/blog/abnormal-attack-stories-6-coronavirus-credential-theft/

9. "FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic". 20 de marzo de 2020. FBI.
https://www.ic3.gov/media/2020/200320.aspx

10. "Beware of criminals pretending to be WHO". 2020. OMS. https://www.who.int/about/communications/cyber-security

11. "Global police agencies issue alerts on Covid-related cyber-crime". 6 de abril de 2020. SC Magazine.
https://www.scmagazineuk.com/global-police-agencies-issue-alerts-covid-related-cyber-crime/article/1679473

12. "Catching the virus cybercrime, disinformation and the COVID-19 pandemic". 3 de abril de 2020. EUROPOL.
https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic

13. "New FireEye Email Threat Report Reveals Increase in Social Engineering Attacks". 25 de junio de 2019. FireEye.
https://www.fireeye.com/company/press-releases/2019/new-fireeye-email-threat-report-reveals-increase-in-social-engin.html

14. "HTTPS Protocol Now Used in 58% of Phishing Websites". 24 de junio de 2019. Trend Micro.
https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/https-protocol-now-used-in-58-of-phishing-websites

15. Let's Encrypt. https://letsencrypt.org/

16. "2020 'State of the Phish': Security Awareness Training, Email Reporting More Critical as Targeted Attacks Spike". 23 de enero de 2020. Proof Point. https://www.proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical

17. "Human factor report". 2019. Proof Point. https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf

18. "Phishing Activity Trends Report Q3". 2019. APWG. https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf

19. "Business Email Compromise Results in $26B in Losses Over the Last Three Years". 12 de septiembre de 2019. Proof Point. https://www.proofpoint.com/us/corporate-blog/post/business-email-compromise-results-26b-losses-over-last-three-years

20. "Business Email Compromise The $26 Billion Scam", 10 de septiembre de 2019. FBI. https://www.ic3.gov/media/2019/190910.aspx

21. "Evasive Phishing Driven by Phishing-as-a-Service". 1 de julio de 2019. Cyren.

https://www.cyren.com/blog/articles/evasive-phishing-driven-by-phishing-as-a-service

22. "Phishing made easy: Time to rethink your prevention strategy?". 2016. Imperva. https://www.imperva.com/docs/Imperva-HII-phishing-made-easy.pdf

23. "Q3 2019: Email Fraud and Identity Deception Trends". 2019. Agari. https://www.agari.com/insights/ebooks/2019-q3-report/

24. "FBI: BEC Losses Soared to $1.8 Billion in 2019". 12 de febrero de 2020. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/fbi-bec-losses-soared-to-18/

25. "Email: Click with Caution". Junio de 2019. Cisco. https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf

26. "Experts report a rampant growth in the number of malicious, lookalike domains". 18 de noviembre de 2019. https://securityaffairs.co/wordpress/94021/hacking/lookalike-domains-tls-certificate.html

27. "Proofpoint Q3 2019 Threat Report — Emotet's return, RATs reign supreme, and more". 7 de noviembre de 2019. Proof Point. https://www.proofpoint.com/us/threat-insight/post/proofpoint-q3-2019-threat-report-emotets-return-rats-reign-supreme-and-more

28. "Human Factor Report." 2019. Proof Point. https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf

29. "2019 Phishing and fraud report" 2019. F5 Labs. https://www.f5.com/content/dam/f5-labs-v2/article/pdfs/F5Labs_2019_Phishing_and_Fraud_Report.pdf

30. "Report: Microsoft, PayPal, and Netflix Most Impersonated Brands in Phishing Attacks in Q1 2019". 8 de mayo de 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/report-microsoft-paypal-and-netflix-most-impersonated-brands-in-phishing-attacks-in-q1-2019

31. "Spam and phishing in Q3 2019". 26 de noviembre de 2019. Kaspersky. https://securelist.com/spam-report-q3-2019/95177/

32. "Phishing Activity Trends Report". 2019. APWG. https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf

33. "Toyota Subsidiary Loses $37 Million Due to BEC Scam" 20 de septiembre de 2019. CPO Magazine. https://www.cpomagazine.com/cyber-security/toyota-subsidiary-loses-37-million-due-to-bec-scam/

34. Open SPF. http://www.openspf.org/

35. "Domain-based Message Authentication, Reporting & Conformance". DMARC. https://dmarc.org/

Bibliografía

36. "DomainKeys Identified Mail (DKIM)". DKIM. http://www.dkim.org/

37. "Cyber incident". 22 de julio de 2019. Lancaster University. https://www.lancaster.ac.uk/news/phishing-attack

38. "Hackers publish login credentials of 2500 Discord users". 22 de julio de 2019. Cyware Social. https://cyware.com/news/hackers-publish-login-credentials-of-2500-discord-users-8d3ea2c7

39. "Bodybuilding.com Breach: Proof That An Organization's Biggest Cyber Risk Is Its People". 24 de abril de 2019. Forbes. https://www.forbes.com/sites/jameshadley/2019/04/24/bodybuilding-com-breach-proof-that-an-organizations-biggest-cyber-risk-is-its-people/#1ea113751bef

40. "Phishing Attack Exposes 600k Health Records". 19 de junio de 2019. Secure World. https://www.secureworldexpo.com/industry-news/healthcare-data-breach-example-2019

41. "326,000 Patients Impacted in UConn Health Phishing Attack". 25 de febrero de 2019. Health IT Security. https://healthitsecurity.com/news/326000-patients-impacted-in-uconn-health-phishing-attack

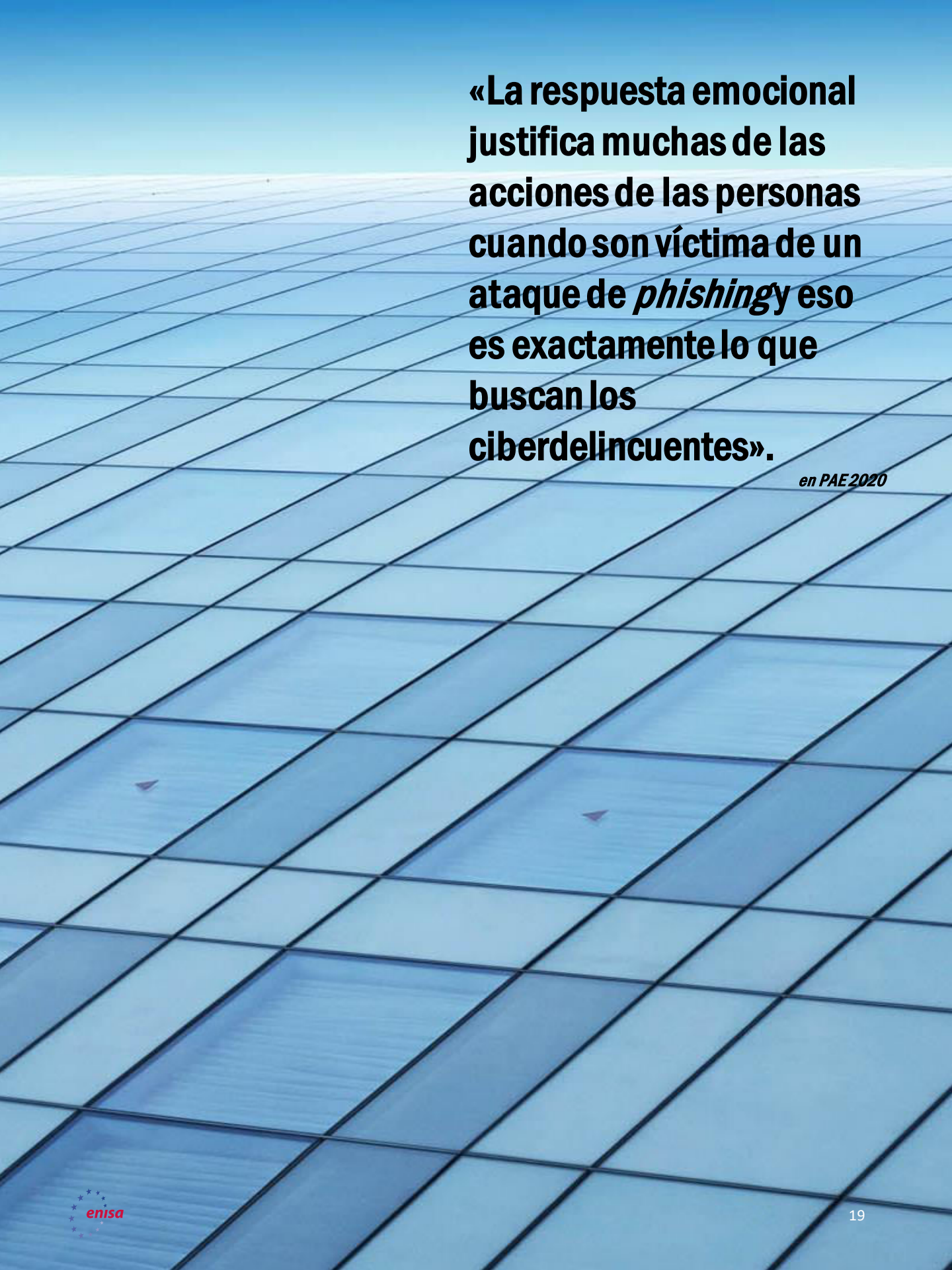
42. "Cybercrime Tactics and Techniques: the 2019 state of healthcare". 2019. Malwarebytes. https://resources.malwarebytes.com/resource/cybercrime-tactics-and-techniques-the-2019-state-of-healthcare/

43. "Significant Cyber Incidents". 2019. CSIS. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

44. "More Than 99% of Cyberattacks Need Victims' Help". 9 de septiembre de 2019. Dark Reading. https://www.darkreading.com/cloud/more-than-99--of-cyberattacks-need-victims-help/d/d-id/1335769

45. "office-365-phishing-attacks-deconstructed" https://dropsuite.com/office-365-phishing-attacks-deconstructed/

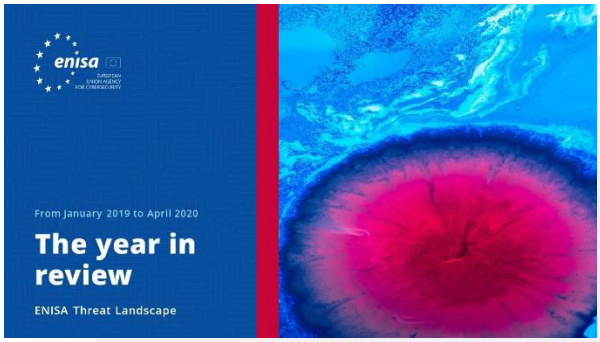
46. ENISA. https://www.enisa.europa.eu/topics/wfh-covid19



«La respuesta emocional justifica muchas de las acciones de las personas cuando son víctima de un ataque de *phishing* y eso es exactamente lo que buscan los ciberdelincuentes».

en PAE 2020

Lecturas relacionad



LEER EL INFORME

Informe Panorama de Amenazas de la ENISA **Revisión anual**

Un resumen de las tendencias en materia de ciberseguridad durante el período de enero de 2019 a abril de 2020.

LEER EL INFORME

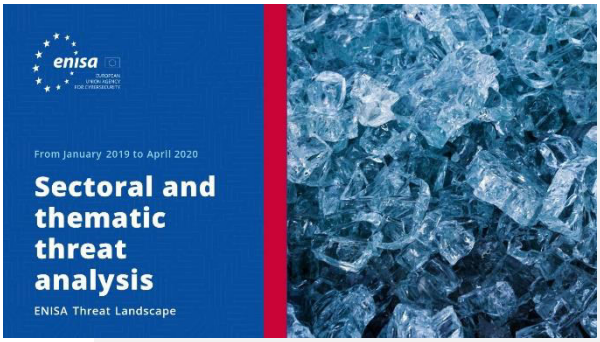
Informe Panorama de Amenazas de la ENISA
Lista de las 15 amenazas principales

Lista de la ENISA con las 15 amenazas principales durante el período de enero de 2019 a abril de 2020.

LEER EL INFORME

Informe Panorama de Amenazas de la ENISA
Temas de investigación

Recomendaciones sobre temas de investigación de varios cuadrantes de la ciberseguridad y de la inteligencia sobre las ciberamenazas.



LEER EL INFORME

Informe Panorama de Amenazas de la ENISA **Análisis de las amenazas por sectores y temas**

Análisis contextualizado de las amenazas durante el período de enero de 2019 a abril de 2020.

LEER EL INFORME

Informe Panorama de Amenazas de la ENISA **Tendencias emergentes**

Principales tendencias en ciberseguridad observadas entre enero de 2019 y abril de 2020.

LEER EL INFORME

Informe Panorama de Amenazas de la ENISA
Sinopsis de la inteligencia sobre las ciberamenazas

Situación actual en materia de inteligencia contra las ciberamenazas en la UE.

¿Quiénes somos?

_ La agencia

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) es la agencia de la Unión cuyo objetivo es alcanzar un elevado nivel común de ciberseguridad en toda Europa. La agencia se estableció en 2004, se ha visto reforzada por el Reglamento sobre la Ciberseguridad y contribuye a la política cibernética de la UE, mejora la fiabilidad de los productos, servicios y procesos de TIC con programas de certificación de la ciberseguridad, coopera con los Estados miembros y los organismos de la UE y ayuda a Europa a prepararse para los desafíos cibernéticos del futuro. A través del intercambio de conocimientos, la capacitación y la sensibilización, la Agencia coopera con sus partes interesadas clave para fortalecer la confianza en la economía conectada, para impulsar la resiliencia de la infraestructura de la Unión y, por último, para proteger digitalmente a la sociedad y a la ciudadanía de Europa. Puede encontrarse más información sobre la ENISA y su labor en www.enisa.europa.eu.

Colaboradores

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) y *todos los miembros del grupo de partes interesadas de la CTI (inteligencia sobre las ciberamenazas) de la ENISA:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) y Thomas Hemker.

Editores

Marco Barros Lourenço (ENISA) y Louis Marinos (ENISA).

Datos de contacto

Las consultas acerca de este informe deben realizarse a través de enisa.threat.information@enisa.europa.eu.

Las consultas de los medios de comunicación acerca de este informe deben realizarse a través de press@enisa.europa.eu.

Nos gustaría conocer su opinión sobre este informe

Le pedimos que dedique unos minutos a rellenar el cuestionario. Para acceder al cuestionario haga clic aquí.

Aviso legal

Salvo que se indique lo contrario, la presente publicación refleja las opiniones e interpretaciones de la ENISA. Esta publicación no constituye en ningún caso una medida legal de la ENISA ni de los organismos que la conforman, a menos que se adopte en virtud del Reglamento (UE) 526/2013. La información tampoco refleja necesariamente el estado actual de la técnica y la ENISA se reserva el derecho a actualizarla en todo momento.

Las correspondientes fuentes de terceros se citan cuando proceda. La ENISA declina toda responsabilidad por el contenido de las fuentes externas, incluidos los sitios *web* externos a los que se hace referencia en esta publicación.

Esta publicación tiene un carácter meramente informativo. Además, debe poder accederse a la misma de forma gratuita. Ni la ENISA ni ninguna persona que actúe en su nombre aceptan responsabilidad alguna en relación con el uso que pueda hacerse de la información incluida en la presente publicación.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grecia
Tel.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu