IN THIS ISSUE...

02
COVID-19
What’s Trending

03
Service Spotlight
Complex Investigations & Litigation

04
A Look Back & Ahead
Recent & Upcoming Events

05
In Case You Missed It
Thought Leadership
COVID-19 TRENDING
DAMAGING POTENTIAL OF ‘PHONE SPEAR PHISHING’

The infamous Twitter hack that occurred in mid-July and targeted more than a hundred accounts of high-profile individuals was accomplished through ‘voice phishing,’ a methodology that has existed for years. This simple, but effective, technique relies on social engineering – manipulating individuals to divulge confidential information.

Concerningly, “in just the past month since the Twitter hack unfolded, dozens of companies…have been targeted with the same hacking playbook” (WIRED). Cyber actors are taking what they learned from the Twitter hack and replicating it to target other organizations, who are perhaps more vulnerable due to remote working conditions from the COVID-19 pandemic. With much of the world’s workforce operating outside of traditional offices, social engineering attacks have become more difficult to defend.

Furthering the issue, these voice phishing attacks seem to be well-coordinated and researched. Cyber actors are leveraging social media and other publicly available information to build a target list aimed at recent hires to exploit their inexperience. While the Twitter hack was allegedly orchestrated by teenagers, it’s plausible to expect cyber criminal organizations or even nation-state actors to copy and improve upon successful tactics.

Combatting social engineering attacks requires a staff that is cyber aware, which can be accomplished through tailored training. This will help build employees’ knowledge base, define appropriate standards of behavior, and promote secure conduct.

HOW FTI CYBERSECURITY CAN HELP
FTI Cybersecurity builds a safer future by helping organizations understand their own environments, harden their defenses, rapidly and precisely hunt threats, holistically respond to crises, and sustainably recover their operations and reputation after an incident.
SERVICE SPOTLIGHT
COMPLEX INVESTIGATIONS & LITIGATION

UNIQUELY EQUIPPED TO SOLVE COMPLEX PROBLEMS
Our team routinely tackles global, large-scale, and complex issues, that often stem from data security related concerns and demand intricate solutions. We quickly unearth key facts and data sets to enable timely and strategic decisions in investigations, leading to cutting-edge and data-driven results.

CUSTOMIZED APPROACH & SOLUTIONS
FTI Consulting offers creative solutions customized to the industry, size, and challenge specific to the client, and our teams consists of industry and technology experts that apply real-world expertise and proven strategies to tackle any issue. Further, we use tailored advanced analytics capabilities leveraging artificial intelligence, machine learning, and data mining technologies to deliver for our clients.

SELECT EXPERIENCE

CYBER VULNERABILITIES INVESTIGATION
Following an internal investigation at a multi-billion dollar energy-sector business, we identified several cyber vulnerabilities at the company. We prepared and presented a cybersecurity assessment and a remediation plan to the company’s CEO and Board of Directors. In addition, after designing and implementing a cost-effective monitoring program, we identified two employees who were actively stealing trade secrets. The information developed by our investigation led to successful motions for injunctive relief and to the recovery of the stolen proprietary information. We also coordinated successful referrals to federal law enforcement.

ATTRIBUTION OF FRAUDULENT MALWARE CAMPAIGNS
We were hired by a telecom company to investigate web hosting providers suspected of supporting malicious cyber campaigns related to bank and advertising fraud. Our experts used machine learning and sophisticated data aggregation, correlation, and analytic techniques to map millions of IP addresses and hundreds of thousands of URL’s associated with the plaintiff’s hosting infrastructure back to historical malicious applications and botnet activity. After the investigation was complete, we provided step-by-step examples to counsel showing corroboration of claims by the client, including systemic evidence of malicious cyber activity supported and facilitated by the client’s business.

If you would like to learn more, please email #FTICybersecurity.
A LOOK BACK & AHEAD

RECENT EVENTS

SOUTH AFRICA WEBINAR
July 30 | Virtual
FTI Consulting’s Caroline Parker and Geoff Budge and speakers highlighted how South African businesses are unprepared for the fallout from cyber attacks. Watch the webinar recording here.

ABA CYBERSECURITY, PRIVACY AND DATA PROTECTION COMMITTEE
August 4 | Virtual
The ABA Cybersecurity, Privacy and Data Protection Committee hosted a webinar covering the latest in cyber-related litigation and incident response best practices. Global Head of Cybersecurity Anthony J. Ferrante was a panelist.

THE CYBERSECURITY WAR ROOM: PRACTICING YOUR RESPONSE TO THE FIRST SEVEN DAYS OF A BREACH
August 4 & 12 | Virtual
Senior Managing Director Ron Yearwood participated in a virtual two-part workshop that walked through threat scenarios and taught attendees how to develop the ideal response.

CYBERSECURITY: TRENDS AND THREATS FOR JAPANESE MULTINATIONAL CORPORATIONS
August 6 | Virtual
Kyung Kim, Head of Cybersecurity APAC, was joined by Joanne Wong (SMD, SC) and Maiko Morikawa (SD, SC) to record a webinar for the Japanese Institute for Overseas Investment (JOI). The recording will be available on JOI’s members-only website from mid-August until early September.

UPCOMING EVENTS

FTI CONSULTING CPD DAY
September 9 & 16 | Virtual
FTI Consulting will be hosting a virtual CPD Day, split across two sessions. The first session, ‘Cybersecurity – Defending Your Company & Keeping Up To Date With Key Risks in 2020’ will be delivered by Head of Cybersecurity, APAC Kyung Kim, and the second session ‘Data Breach & Crisis Management’ will be co-presented by Kyung Kim & Joanne Wong.

STANFORD UNIVERSITY CYBER POLICY, RISK AND SECURITY EXECUTIVE EDUCATION PROGRAM
September 30 | Virtual
Head of Cybersecurity for the Americas, Jordan Rae Kelly will teach a module at Stanford’s four-day program. Learn more here.
IN CASE YOU MISSED IT

THOUGHT LEADERSHIP

THE EXPERT BRIEFING PODCAST SERIES
FTI Cybersecurity’s global podcast series ‘The Expert Briefing’ is now live across Apple, Google, and Spotify stores. Cybersecurity is always evolving, and we will be adding new episodes regularly discussing the latest industry trends. Listen here.

REBUILDING TRUST AFTER A CYBER ATTACK
Authored by Managing Directors Caroline Parker (SC) and Geoff Budge (TECH), this article discusses why increased business vulnerability amplifies the need for companies to carefully consider their ability to respond effectively. Click to read.

NOT IF, BUT WHEN: BUILDING CYBERSECURITY RESILIENCE TO SECURE COMPETITIVE ADVANTAGE
Authored by Joshua Burch, Head of Cybersecurity, EMEIA, this paper covers tangible actions that boards and business leaders should take to develop their cybersecurity resilience. Click to read.

FOR MORE INFORMATION

To learn more about FTI Cybersecurity, please visit: www.fticybersecurity.com

Follow us on Twitter! @FTICyber

The FTI Cybersecurity Briefing Book is your monthly window into the latest news from around the industry and highlights from FTI Cybersecurity. The Cybersecurity Briefing Book provides team and service offering updates, as well as trends that we are identifying that may affect your practices and clients. We also highlight case studies that show the depth, scope, and nature of work that we do for clients.

About FTI Cybersecurity
FTI Cybersecurity’s structure and capabilities are engineered to synthesize cutting-edge intelligence-led cybersecurity practices around a trusted core of comprehensive offerings. Our team enables clients of any size to address their most critical needs and integrate new solutions atop or alongside any preexisting policies and programs.