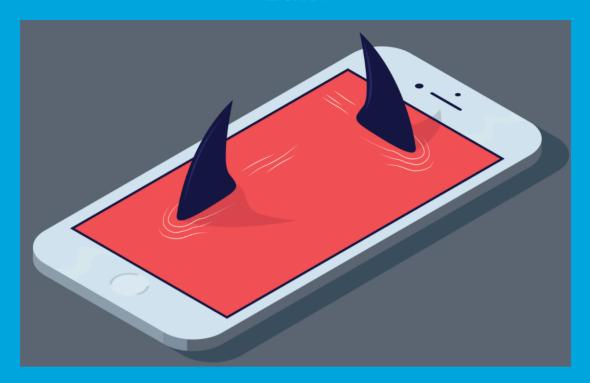# Security Newsletter

27 Avril 2020

Subscribe to this newsletter

When in Doubt: Hang Up, Look Up, & Call Back

Many security-conscious people probably think they'd never fall for a phone-based phishing scam. But if your response to such a scam involves anything other than hanging up and calling back the entity that claims to be calling, you may be in for a rude awakening. Here's how one security and tech-savvy reader got taken for more than $10,000 in an elaborate, weeks-long ruse.

Mitch's bank managed to reverse the unauthorized wire transfer before it could complete, and they've since put all the stolen funds back into his account and issued a new card. But he said he still feels like a chump for not observing the golden rule: If someone calls saying they're from your bank, just hang up and call them back — ideally using a phone number that came from the bank's Web site or from the back of your payment card. As it happened, Mitch only followed half of that advice

As Mitch's experience shows, many security-conscious people tend to focus on protecting their online selves, while perhaps discounting the threat from less technically sophisticated phone-based scams. In this case, Mitch and his bank determined that his assailants never once tried to log in to his account online. "What's interesting here is the entirety of the fraud was completed over the phone, and at no time did the scammers compromise my account online," Mitch said. "I absolutely should have hung up and initiated the call myself. And as a security professional, that's part of the shame that I will bear for a long time."

Read More

More #News

- 309 million Facebook users' phone numbers found online
- Chinese Hackers Using New iPhone Hack to Spy On Uyghur Muslims
- Nintendo says 160,000 users impacted in recent account hacks
- 267 million Facebook profiles sold for $600 on the dark web
- Phishing uses lay-off Zoom meeting alerts to steal credentials
- Phishing attacks target US Payroll Protection Program Loans
- Malicious USB Drives Infect 35,000 Computers With Crypto-Mining Botnet
- This is how viewing a GIF in Microsoft Teams triggered account hijacking bug
- New GreyNoise free service alerts you when your devices get hacked

#Patch Time!

- Apple Rushes to Patch iOS Zero-Day Flaws
- Microsoft Teams patched against image-based account takeover
- Critical bug in Google Chrome – get your update now
- Patch now! Microsoft issues unexpected Office fix
- Hackers exploit zero-day in Sophos XG Firewall, fix released

#Tech and #Tools

- You've Got (0-click) Mail! - iOS exploit write-up
- Hunting for credentials and building a credential type reference catalog
- The Extended AWS Security Ramp-Up Guide
- Azure AD Introduction for Red Teamers
- Malware development part 1
- OWASP Web Security Testing Guide v4.1 release
- Burp extension generator
- Red Team Tactics: Utilizing Syscalls in C# - Prerequisite Knowledge
- Abusing Firefox in Enterprise Environments
- Open Redirects - Everything That You Should Know
- Anatomy of Automated Account Takeovers
- Everything You Need to Know About IDOR (Insecure Direct Object References)
- Open-Source SOAR Solution : Part 1
- A Defender's Guide For Rootkit Detection: Episode 1 – Kernel Drivers
- Jamfing for Joy: Attacking macOS in Enterprise

This content was created by [Kindred Group Security](). Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at [https://news.infosecgur.us]()