WEEKLY THREAT BRIEF

Signal & Noise

RADICL™
radicl.com
vSOC PUBLICATION
ISSUE 06 · WEEK OF AUG 10, 2026

FIELD GUIDE

What Is Phishing, Really?

Everyone has heard the word. Far fewer can say what a phishing email is actually trying to get out of them, or why the good ones look nothing like the examples in your annual training.

Phishing is any message engineered to make you act against your own interest: hand over a password, approve a login, open a file, pay an invoice. It is not a technical attack. It is a social one that happens to arrive by email. Nobody is breaking your inbox; they are borrowing your habits.

01
RECON
Real names, real programs, real contract numbers. Pulled from public sites and a partner's stolen mail.

02
TRUST
A reply in a thread you started, or a mailbox that really does belong to your supplier. Filters see a friend.

03
THE ASK
Do something now, quietly, outside how you normally do it. Urgency plus a shortcut around process.

04
PAYOFF
A wire in the wrong account, a session token, or remote access that outlives the email.

STOP HUNTING FOR TYPOS

The badly spelled version still exists, and it is not what we worry about. The good ones are polished, in-thread, and specific to your program.

Which is why "we have a filter" is not a plan: **a reply inside an existing conversation almost never gets flagged**.

DO THIS INSTEAD: S.T.A.R.

- **S** **Stop.** Urgency is the attack. Nothing legitimate dies in five minutes.
- **T** **Think about the ask.** Payment change, password, approval, install?
- **A** **Ask on another channel.** Call the person. Never verify by reply.
- **R** **Report it** while it is still a question. Especially if you clicked.

One message. One click. One decision you get to make slowly.

IN THIS ISSUE

THIS WEEK IN CYBER HISTORY

AUG 15, 2012

Shamoon Wipes 30,000 Workstations

A crude wiper erased the hard drives of most of Saudi Aramco's office fleet in hours. The malware wasn't sophisticated. The flat network was.

ANATOMY OF THE ASK

Credential harvest
A login page reached by link, not bookmark, collecting your password

MFA fatigue
Repeat approval prompts you never triggered

Thread hijack
A reply inside a real conversation you started

Payment redirect
New bank details on a familiar invoice

Silent install
An attachment that runs remote-access software

WHY THIS MATTERS

Phishing is still how most intrusions start, and defense suppliers are a deliberate target: the same program data a prime protects sits in the inboxes of far smaller companies. Attackers go where the **trust is real and the tooling is thinner**.

You are not expected to spot every fake, and we are not grading you. Slow down on the ask, flag the ones that feel off. Filters catch strangers; people and analysts catch the mail that shows up already trusted.

MEET THE ANALYST

Maya Douglas

SOC ANALYST II

Maya's security career began during her CS undergrad at CU Boulder and has spanned contracting at Microsoft and running cybersecurity for MSPs. Four years writing for Her Campus means she came into security already knowing how to tell a story.

A Girl Security alum, WiCyS member, and CTF designer, she believes the best defenders come from everywhere. RADICL's focus on the underserved Defense Industrial Base fits her passion for SMB security: the segment that gets overlooked, underprotected, and increasingly targeted by nation-states.

> **The companies that get hit hardest are the ones everyone assumes are too small to be a target.**
>
> — MAYA DOUGLAS, SOC ANALYST II · vSOC

CASE SPOTLIGHT

BENIGN · RULE TUNED

A first-seen hardware-inventory query on a developer workstation paged as suspicious recon. Full process ancestry showed a battery-health check from an IDE terminal. Closed benign, and we tuned the rule so it stops firing.

NEVER EXECUTED

A file disguised as a routine coursework template hit a learning platform's upload pipeline carrying a hash reputation already flagged as a known web shell. We traced its process lifecycle and confirmed it never executed.

DRIVER QUARANTINED

A file posing as a .NET Framework installer silently deployed a foreign consumer antivirus suite plus a driver with known vulnerabilities. The driver was quarantined on install; we flagged the rest for removal.

EYE ON THE THREATSCAPE

01 Evil Twin at 30,000 Feet, Post-DEF CON

A rogue "Delta WiFi Fast" network appeared on Flight 591 out of Las Vegas the day after DEF CON. Crew killed in-flight Wi-Fi for 30 minutes and the feds are investigating. Classic evil twin: a network that looks like the one you expected, run by someone who wants your session. Same lure as email phishing, different delivery.

02 One Invisible Pixel, Full Dev Access

Researchers hid one-pixel text on a web page that made an AI coding assistant rewrite its own config and launch an attacker-controlled server with developer privileges. Nobody clicked anything. It is patched, but the pattern is the story: an agent that reads the web will read instructions planted there too.

03 Know Every Supplier In Your Software

A new executive order pushes end-to-end visibility into defense supply chains: software dependencies, foreign ownership, supplier risk. Expect the questions to reach subcontractors long before any rule does, and expect primes to ask for answers in writing.

VSOC TIP OF THE WEEK

If a download or install prompt surprises you, don't click through and don't just dismiss it. Report it. A 10-second heads-up lets us check whether it was a real attempt before the next one lands, and a dismissed prompt tells us nothing.