PRETEXT STORIES

THE SCAM-PROOF KIT
FREE SAMPLE

Five pages from the full kit: two of the 22 Case Files, two pages of word-for-word call-back scripts, and the printable pocket cards.

Get the full kit (57 pages, 6 Word policies, Excel workbook) at pretextstories.com/kit

CASE FILE 12 · 2021

THE UNUSED ACCOUNT

Colonial Pipeline, a network of more than 5,500 miles of pipe carrying fuel from the Gulf Coast to New York Harbor

5,500 mi of pipeline shut down, Colonial says

Colonial's CEO told senators the company believes attackers used a legacy VPN profile that was not meant to be in use.

What happened

1. On May 7, 2021 an employee found a ransom note on a computer in Colonial's IT network. Colonial says the whole pipeline was shut down by ten past six.
2. At a Senate hearing the CEO said the company believes the attackers exploited a legacy VPN profile that was not intended to be in use.
3. Cybersecurity Dive reported the CEO said the profile had no multi-factor authentication, and that the password was complicated.
4. The Justice Department says Colonial paid approximately 75 bitcoins on or about May 8. Pipelines began returning to service on May 12.
5. On June 7 the Justice Department announced a seizure of about 63.7 bitcoins, which it said is alleged to be ransom proceeds.

The gap. A legacy VPN profile nobody meant to use was still live, and its login was the only lock. Per remarks reported by Cybersecurity Dive, it had no multi-factor authentication.

What helped, or would have helped

- The FBI and CISA advisory lists first among its mitigations: require multi-factor authentication for remote access to both IT and OT networks.
- The Justice Department thanked Colonial for quickly notifying the FBI. Colonial says it shut down the legacy VPN profile.
- Common practice: find and remove accounts and profiles nobody uses. An old login is still a login.

RULE 3 · A key beats a code RULE 4 · Two people, least access

☐ **Try this week.** Common practice: this week, list every VPN profile and remote-access account, close any nobody uses, and check that the rest ask for a second step.

Sources: CEO written testimony (June 8, 2021); DOJ press release (June 7, 2021); CISA/FBI advisory AA21-131A; Cybersecurity Dive (June 9, 2021)

CASE FILE 22 · 2016

THE FORGED MESSAGES

Bangladesh Bank, the central bank of Bangladesh; its accounts at the New York Fed

$951M attempted, per the indictment (allegation)

According to a federal indictment, fraudulent payment instructions targeting about $951M were sent; about $81M reached the Philippines. Allegations, not verdicts.

What happened

1. The complaint alleges that in January 2015 emails from a supposed job applicant linked to a resume; at least three bank computers tried to download it.
2. The complaint says a backdoor was saved in the network by March 2015, and intruders moved to the core SWIFT processing system on January 29, 2016.
3. The complaint says attackers crafted messages appearing to come from the bank's system, telling the New York Fed to move dollars to accounts in the Philippines and Sri Lanka.
4. The indictment dates the instructions to February 4, 2016. About $81 million reached the Philippines; the complaint says a recipient bank stopped $20 million sent to Sri Lanka.
5. The complaint alleges malware deleted the fraudulent messages from the SWIFT server database and altered what would otherwise have printed for the bank's records.

The gap. Per the complaint, malware at the bank deleted message records and modified what would otherwise have printed, so the machine that kept the records could not be trusted as proof.

What helped, or would have helped

- SWIFT says fraudulent instructions would show in the correspondent bank's end-of-day statements, so reconcile against a record the attacker cannot reach, such as its Daily Validation Report.
- SWIFT's Payment Controls Service lets a bank require out-of-band confirmation for particular combinations of amounts, currencies or countries.
- SWIFT says without an incident response plan it is near impossible to respond well, so know in advance how to cancel a payment.

RULE 1 · Check on a channel you chose RULE 4 · Two people, least access

☐ **Try this week.** Common practice: for large payments, require a second person and an out-of-band confirmation, and check balances against your bank's statement, not only your own records.

Sources: DOJ press release and criminal complaint (2018); DOJ press release and indictment (2021); SWIFT statements (May 2016); SWIFT ISAC report (Apr 2019); SWIFT CSCF page; New York Fed joint statements (2016, 2019); BAE Systems blog (company analysis)

HOW TO USE THIS PART

SAY IT THE SAME WAY EVERY TIME

Pressure works because people improvise. A script removes the improvising. Read these aloud once, put the ones you need next to the phone, and agree as a team that using them is **normal, not rude**. A real supplier, bank or colleague will never mind a call-back.

> **The one move behind every script:** stop the conversation, then restart it on a channel you chose, using a number you already had.

Contents

1. Someone asks you to change bank details
2. An "executive" asks for an urgent payment or gift cards
3. A caller says they are from IT or the help desk
4. You are the help desk: someone asks for a password or second-step reset
5. Your bank's "fraud department" calls you
6. A text or email says your account will be closed
7. A video call asks you to move money
8. A new supplier or new hire needs to be verified
9. Someone says "don't tell anyone"
0. You realise you already clicked, typed or paid
1. A family member calls in an emergency

THE SCRIPTS

ELEVEN SITUATIONS

1 · Someone asks you to change bank details

By email, call or message. A supplier, a staff member, a landlord, a client. RULE 1 NEW ACCOUNT

> *"Thanks for letting us know. For our records, I'll call you back on the number we already have on file to confirm the change. Payments won't change until I have."*

Then: call the number from your **own** records, never from the message. Ask them to confirm the old account's last four digits and the new details. Get a second person to approve before anything changes (Policy 1).

> **If they push back or get angry:** "I understand it's urgent. It's our standard process for every supplier. I'll do it as soon as the call is done." Pressure to skip the check is a warning sign in itself.

2 · An "executive" asks for an urgent payment or gift cards

A message that looks like it is from the boss: "I'm in a meeting, I need you to handle something confidentially." RULE 1 RULE 4 URGENCY SECRECY

> *"Happy to help. I'll confirm with you on your mobile first, and our process needs a second approver for anything outside the usual."*

Call or message the executive on a number you already have. Never reply to the message. Loop in the second approver. Report the message to your reporting address even if it turns out to be real; your colleagues may get the same one.

3 · A caller says they are from IT or the help desk

They are calling you. They need you to "verify" something, install something, or approve a prompt. RULE 1 RULE 2

> *"I'll hang up and call the help desk back on the number from our company directory. What's your name and ticket number?"*

Hang up. Call the number you already had. If it was a real call, the help desk will confirm it, and nothing is lost. **Never read out a code, approve a prompt you did not start, or type a login into a page they send.**

> **If you are told "it will only take a second":** "No problem. I'll call back and we'll do it then."

4 · You are the help desk: someone asks for a reset

A caller says they have lost their phone, locked their account or need a new second step. RULE 1 RULE 4

> *"To protect your account, I need to verify you first. I'm going to call you back on the number we have on file, and a manager has to approve changes to your sign-in method."*

Follow Policy 3: callback on the number on file, a second approver for any reset of a second step, a short cooling-off before a reset takes effect, and a note to the account owner by a second channel. **Never let the urgency of the caller shorten the procedure.**

PRINT AND CUT

POCKET CARDS

Print on card stock at 100%. Cut along the borders. Give one to every person who touches money, accounts or support.

THE FIVE RULES

1. Check on a channel **you** chose.
2. Never type a login or read out a code because someone asked.
3. A key beats a code.
4. Two people for big actions. Only the access you need.
5. Tell someone fast. It is safe to tell.

FOUR WARNING SIGNS

1. **Urgency.** "Do it now."
2. **Secrecy.** "Don't tell anyone."
3. **A new route for money.** Same supplier, new account.
4. **A fee to get paid.** Pay more to release your own money.

PAUSE: FIVE QUESTIONS

1. Did **I** start this contact?
2. Is there a deadline or a secret?
3. Is it about money, a login or a code?
4. Can I confirm it on a channel I chose?
5. Would a second person say yes?

IF IT GOES WRONG

1. Tell: _____
2. Phone: _____
3. Email: _____
4. Money moved? Call the bank now.
5. Keep the message. Don't delete it.

No blame for reporting. Ever.

Print one set per person. Write your reporting contact in the "If it goes wrong" card before printing.