Fable Security

By Dr. Sanny

One ish two ish

How to neutralize modern phishing

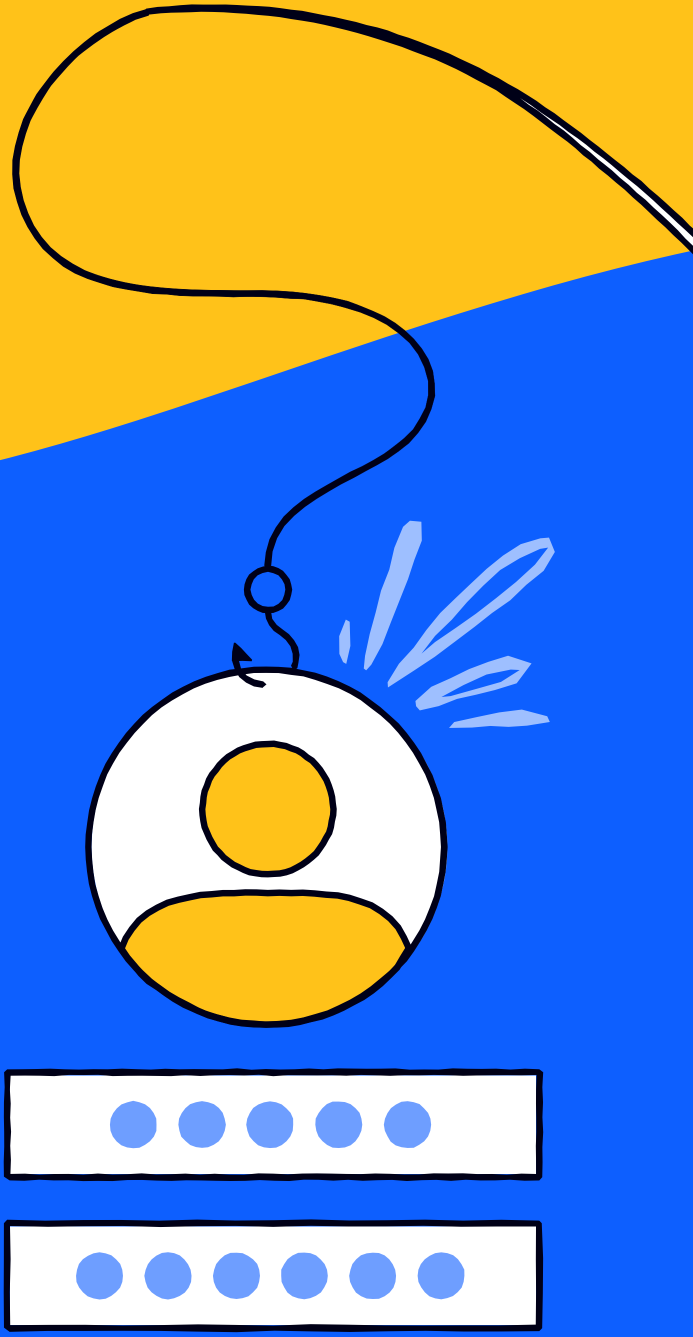


Table of contents

Why this book

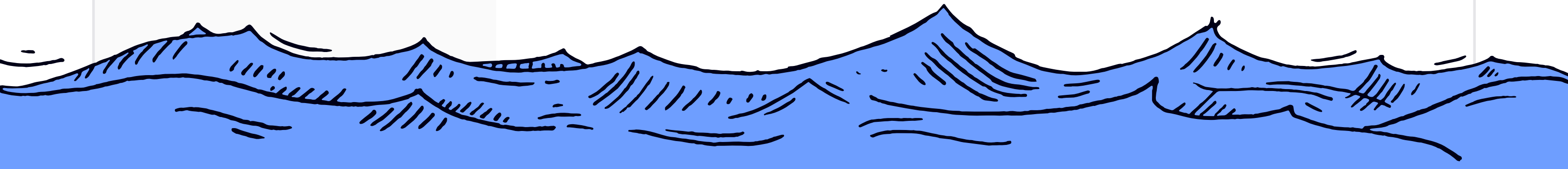
Social engineering is the most effective way into your organization today. This eBook breaks down the tricks they use to exploit the people in your company, and how to prevent, contain, and remediate them.

What do we mean by "ishing"? "Ishing" is a catch-all for the modern spin-offs of phishing—tricks that fool people into clicking, leaking, or doing something they'll regret. Whatever the "ish," it always ends with trouble.

What follows are 17 high-value "ishes" we've seen plague enterprises and a high-level checklist for how to neutralize them (before, during, or after an attack). Note: This checklist is a quick reference; most companies have detailed protocols tailored to their business. Further, our containment and remediation advice may vary depending on people's level of engagement with the attack.

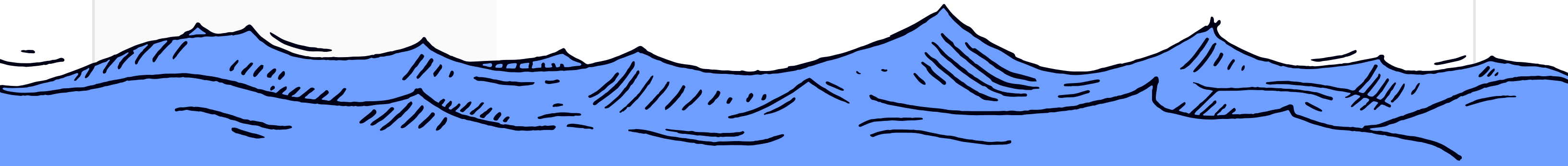
Phishing

Delivery method	Email, phone, text, messaging apps, business apps, social media
Description	Emails or other messages that trick victims into clicking on malicious links or attachments that can lead to credential compromise, malware installation, or other fraud.
How to prevent	• Train people not to click on suspicious links or attachments • Scrub personal and org chart data from data brokers and public sources • Enforce phishing-resistant MFA on both corporate and personal accounts • Deploy advanced email and web filtering tools • Implement URL rewriting solution
How to contain	• Stop interacting • Alert security • Save message and sender details • Potentially isolate device
How to remediate	• Block and report sender • Reset passwords and revoke sessions • Block associated IP and email address • Scan device for malware • Monitor network for lateral movement and other suspicious activity
Cohorts most at risk	Privileged users, IT admins, VIPs, executives, executive assistants, developers, help desk employees, money handlers



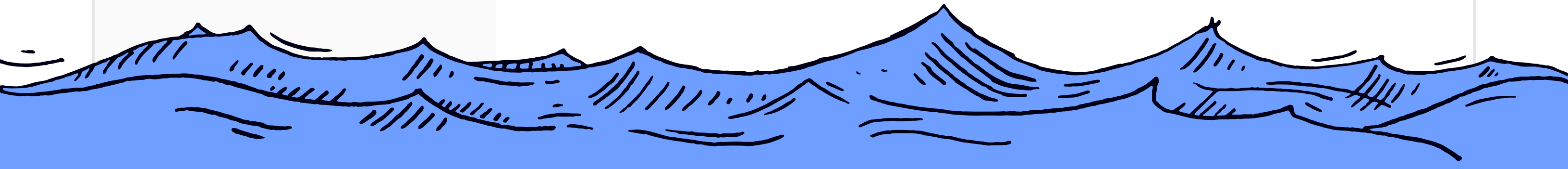
Smishing

Delivery method	Text
Description	Text messages—usually from spoofed numbers—that trick victims into divulging sensitive information, giving system access, or initiating a financial transaction.
How to prevent	• Train people to recognize suspicious or unexpected texts and avoid clicking, replying, or sharing sensitive data • Scrub personal and org chart data from data brokers and public sources • Enable mobile threat defense • Establish verification processes for sensitive requests, like access or payment
How to contain	• Stop interacting • Alert security • Save message or capture screenshots
How to remediate	• Block and report sender • Reset passwords and revoke sessions • Contact financial institution, if applicable • Scan device for malware • Monitor for suspicious activity
Cohorts most at risk	Everyone



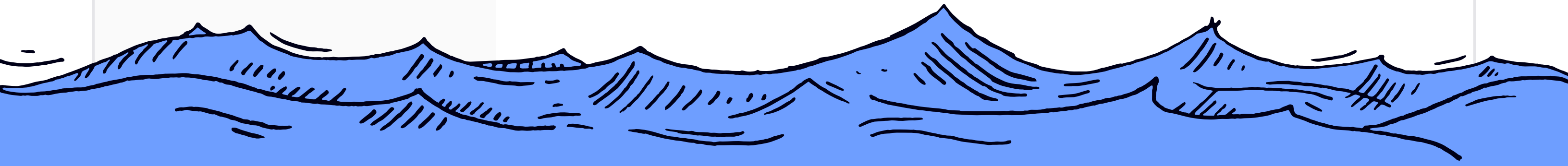
Vishing

Delivery method	Phone
Description	Spoofed phone calls—impersonating a trusted person—that trick victims into divulging sensitive information, giving system access, or initiating a financial transaction.
How to prevent	• Train people to recognize suspicious or high-pressure phone calls and avoid sharing sensitive information • Scrub personal and org chart data from data brokers and public sources • Block calls from unknown numbers • Restrict use of remote access tools • Establish verification processes for sensitive requests, like access or payment
How to contain	• End call • Alert security • Document phone number, time, and call specifics
How to remediate	• Block and report numbers to mobile carrier • Review call logs • Monitor for suspicious activity
Cohorts most at risk	IT admins, help desk employees, money handlers



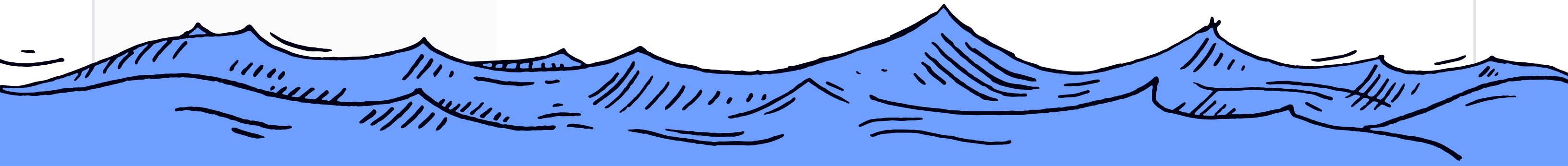
Quishing

Delivery method	QR codes on posters, video, email
Description	Malicious QR codes that trick victims into visiting fake websites or downloading malware.
How to prevent	• Train people not to scan QR codes from unfamiliar sources • Enforce phishing-resistant MFA on both corporate and personal accounts • Enable mobile threat defense • Restrict QR codes in official communications, unless verified and secured • Encourage use of official apps or bookmarked sites
How to contain	• Stop interacting • Alert security • Capture QR code source (e.g., photo or note) • Potentially isolate device
How to remediate	• Reset passwords and revoke sessions • Scan device for malware • Monitor network for lateral movement and other suspicious activity
Cohorts most at risk	Everyone



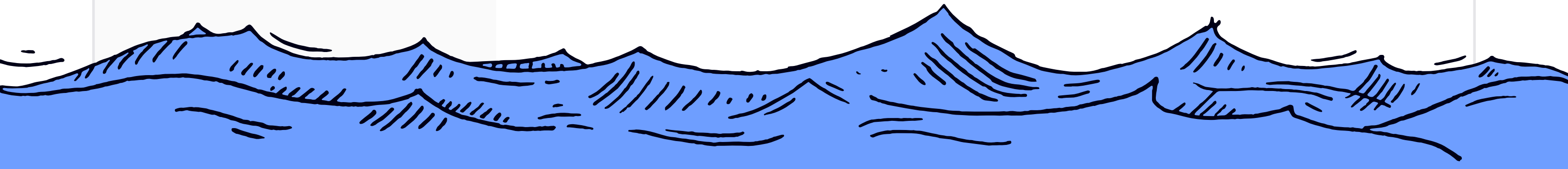
WhatsApp phishing

Delivery method	WhatsApp (messaging and voice notes)
Description	Messages impersonating a trusted contact or business that trick victims into divulging sensitive information, giving system access, initiating a financial transaction, or downloading malware
How to prevent	• Train people to be cautious of unexpected or urgent messages, even from known contacts, and not to click on suspicious links • Scrub personal and org chart data from data brokers and public sources • Enforce phishing-resistant MFA on both corporate and personal accounts • Set messaging app policies to discourage sensitive business communications • Disable link previews where possible • Establish verification processes for sensitive requests, like access or payment
How to contain	• Stop interacting • Alert security • Save message or capture screenshots • Potentially isolate device
How to remediate	• Reset passwords and revoke sessions • Block impersonators • Audit contact list • Scan device for malware • Monitor network for lateral movement and other suspicious activity
Cohorts most at risk	Everyone



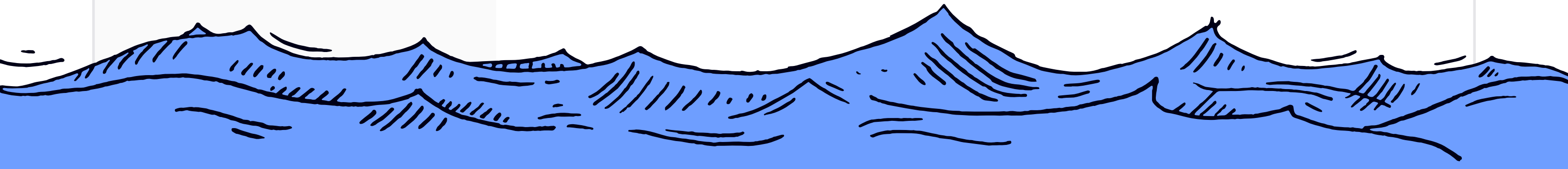
Calendar invite phishing

Delivery method	Calendar invites
Description	Invites auto-added to calendars that trick people into clicking malicious links or attachments.
How to prevent	• Train people to be cautious of unsolicited calendar invites, especially with links or attachments • Scrub personal and org chart data from data brokers and public sources • Configure calendar settings to prevent auto-adds • Establish verification processes for time-sensitive or action-oriented meeting requests
How to contain	• Stop interacting • Alert security • Screenshot sender details • Delete invite • Potentially isolate device
How to remediate	• Reset passwords and revoke sessions • Clear malicious invites • Audit contact list • Scan device for malware • Monitor network for lateral movement and other suspicious activity
Cohorts most at risk	Privileged users, IT admins, VIPs, executives, executive assistants, developers, help desk employees, money handlers



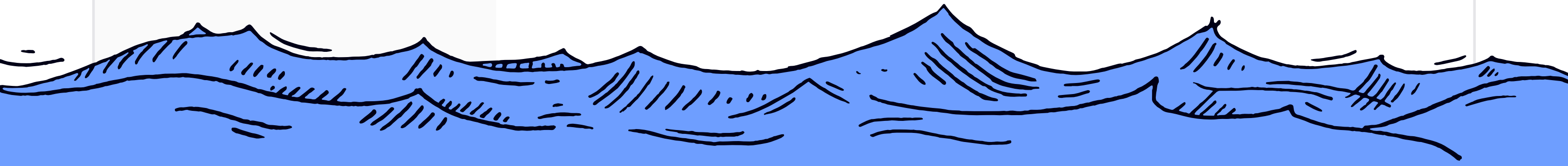
SIM swapping/phone porting

Delivery method	Phone
Description	Sophisticated takeover of a trusted person's phone number—often combined with voice cloning—that tricks victims into divulging sensitive information, giving system access, or initiating a money transfer.
How to prevent	• Train people to be cautious of unexpected phone-related account issues or requests • Scrub personal and org chart data from data brokers and public sources • Enforce phishing-resistant MFA on both corporate and personal accounts • Use carrier PINs or port-out protection • Block calls from unknown numbers • Monitor for SIM changes or unusual activity • Establish verification processes for sensitive requests, like access or payment
How to contain	• Stop interacting • Alert security • Document phone number, time, and call specifics • Contact mobile carrier to lock or recover number
How to remediate	• Review call logs • Notify carrier and financial institution • Monitor for suspicious activity
Cohorts most at risk	Privileged users, IT admins, VIPs, executives, executive assistants, developers, help desk employees, money handlers



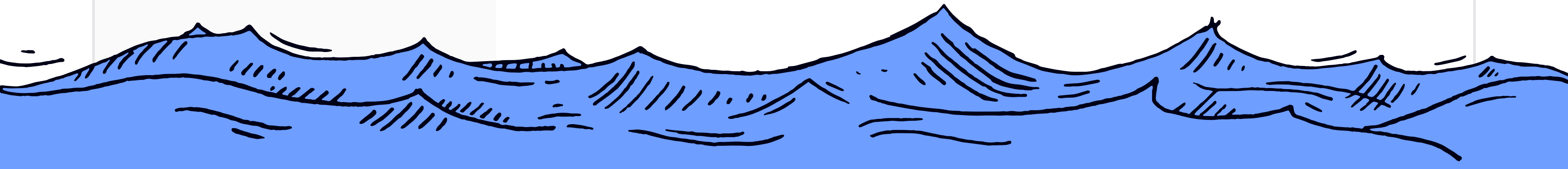
MFA bombing

Delivery method	Push requests, text, email
Description	Notifications from attackers who've stolen credentials that trick people into accepting MFA access requests.
How to prevent	• Train people to recognize, deny, and report repeated or unexpected MFA requests • Scrub personal and org chart data from data brokers and public sources • Enforce phishing-resistant MFA on both corporate and personal accounts • Monitor for use of compromised credentials • Limit MFA attempts allowed within time window • Detect and block suspicious logins
How to contain	• Alert security • Potentially isolate device • Reset passwords and revoke sessions
How to remediate	• Reset passwords and revoke sessions (yes, again) • Scan device for malware • Monitor network for suspicious successful logins across all critical apps • Monitor network for lateral movement and other suspicious activity
Cohorts most at risk	Everyone



Pretexting

Delivery method	Email, phone, text, messaging apps, business apps, social media
Description	Spoofed messages impersonating a trusted contact or business that trick victims—based on a believable scenario—into divulging sensitive information, giving system access, or initiating a financial transaction.
How to prevent	• Train people to be skeptical of urgent or unusual requests • Scrub personal and org chart data from data brokers and public sources • Enforce phishing-resistant MFA on both corporate and personal accounts • Restrict remote access tools • Establish verification processes for sensitive requests, like access or payment
How to contain	• Stop interacting • Alert security • Save message or capture screenshots
How to remediate	• Block caller or sender • Review call logs, if applicable • Notify carrier and/or financial institution, if applicable • Monitor for suspicious activity
Cohorts most at risk	Privileged users, IT admins, VIPs, executives, executive assistants, developers, help desk employees, money handlers

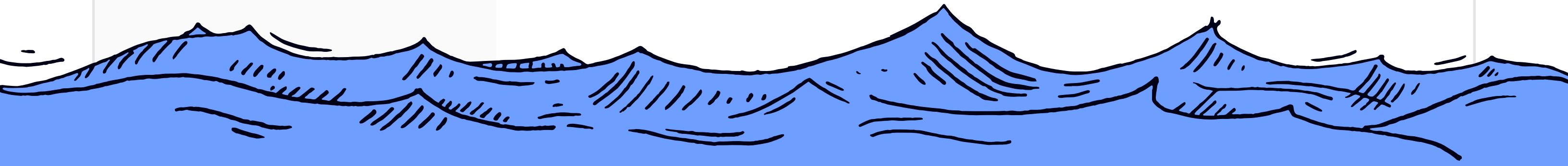


Executive impersonation

Delivery method	Email, phone, text, messaging apps, business apps
Description	Spoofed messages impersonating an executive that trick victims into divulging sensitive information, giving system access, or initiating a financial transaction.
How to prevent	• Train people to be cautious of urgent or high-pressure requests from executives • Scrub personal and org chart data from data brokers and public sources • Use email authentication protocols (e.g., DMARC, DKIM, SPF) to prevent spoofing • Block calls from unknown numbers • Establish verification processes for sensitive requests, like access or payment
How to contain	• Stop interacting • Alert security • Capture screenshots or save call details
How to remediate	• Block caller or sender • Review call logs, if applicable • Notify carrier and/or financial institution • Monitor for suspicious activity
Cohorts most at risk	New hires, executive assistants

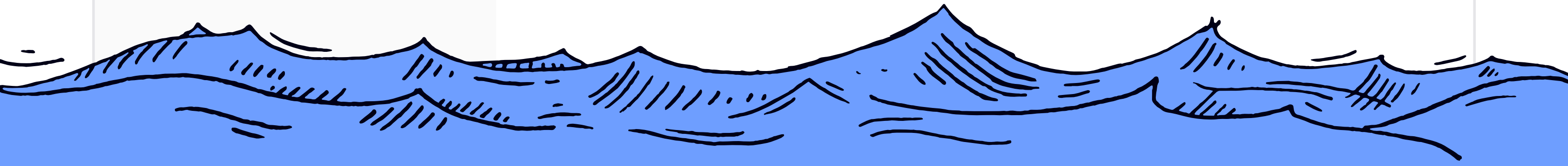
Vendor or invoice fraud

Delivery method	Email, spoofed domains, fake documentation
Description	Spoofed messages impersonating a vendor—or from a compromised vendor account—that trick victims into changing payment information or initiating a financial transaction.
How to prevent	• Train people to be cautious of requests to update vendor payment or banking information • Scrub personal and org chart data from data brokers and public sources • Use email authentication protocols (e.g., DMARC, DKIM, SPF) to prevent spoofing • Maintain a centralized vendor contact directory • Verify vendor details before making changes • Establish change control process in advance that includes out-of-band verification of material changes
How to contain	• Stop interacting • Alert security and finance • Save message or capture screenshots
How to remediate	• Reset vendor details • Add change management checks • Monitor for suspicious activity • Alert vendor and financial institution
Cohorts most at risk	Money handlers, VIPs, executives, executive assistants, vendor managers



Deepfake

Delivery method	Video, audio, or images sent via email, phone, text, messaging apps, video conference apps, business apps, social media
Description	Messages containing AI-generated synthetic media mimicking a real person that trick victims into divulging sensitive information, giving system access, or initiating a money transfer.
How to prevent	• Train people to be skeptical of urgent video or voice requests • Scrub personal and org chart data from data brokers and public sources • Monitor for deepfake impersonation trends targeting people in sensitive roles • Establish out-of-band verification processes for sensitive requests, like access or payment
How to contain	• Stop interacting • Alert security • Capture screenshots or save call details
How to remediate	• Block caller or sender • Review call logs, if applicable • Notify carrier and/or financial institution • Monitor for suspicious activity
Cohorts most at risk	Privileged users, IT admins, VIPs, executives, executive assistants, developers, help desk employees, money handlers



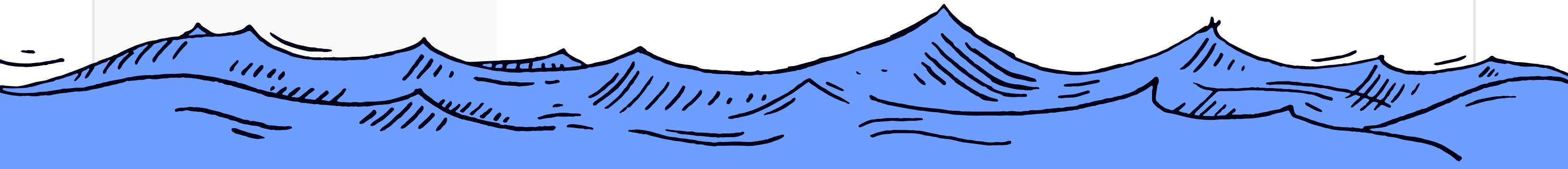
Fable

Scareware

Delivery method	Primarily web
Description	Fake alerts—typically website pop-ups—that trick victims into believing their device is infected or compromised, and then taking action, e.g., downloading malware.
How to prevent	• Train people to ignore alarming pop-ups • Use ad blockers • Enable endpoint protection • Enable automated software updates
How to contain	• Capture screenshots of pop-up • Alert security • Close the browser tab or app • Potentially isolate device
How to remediate	• Reset passwords and revoke sessions • Scan device for malware • Monitor network for lateral movement and other suspicious activity
Cohorts most at risk	Everyone

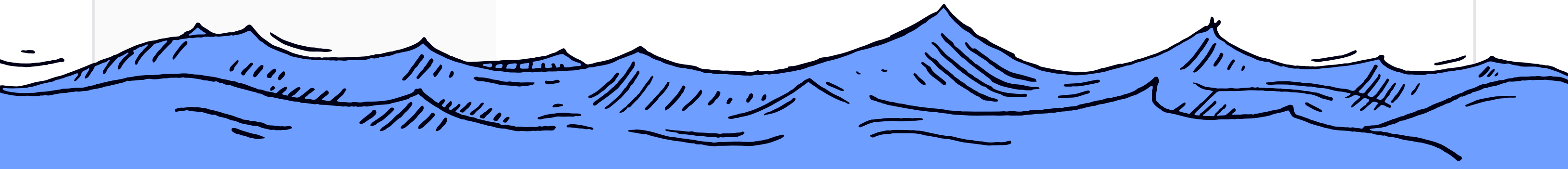
Ransomware

Delivery method	Email, phone, text, messaging apps, business apps, social media
Description	Malware that encrypts files or systems and demands payment—usually in cryptocurrency—for the decryption key.
How to prevent	• Train people not to click on suspicious links or attachments • Scrub personal and org chart data from data brokers and public sources • Segment network and cloud backup services • Enable endpoint protection • Enforce least-privilege admin policies • Ensure regular software updates
How to contain	• Stop interacting • Alert security • Preserve logs and avoid rebooting or tampering with system • Isolate all affected devices
How to remediate	• Wipe and restore machine from backup • Follow response protocol • Reset passwords and revoke sessions • Scan affected devices for malware • Monitor for suspicious activity
Cohorts most at risk	Everyone



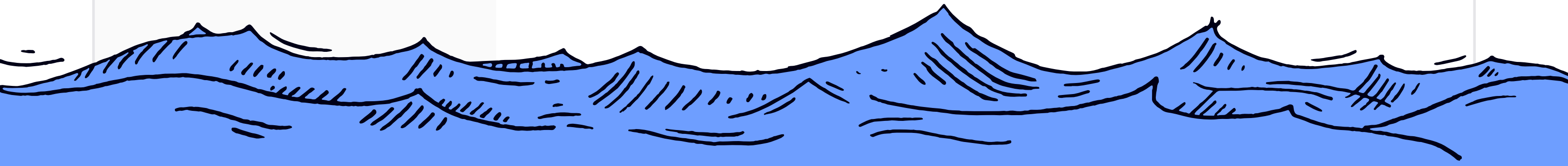
Supply chain attack

Delivery method	Third-party vendors, software updates
Description	Compromise by attackers who've gained access to a victim's device or system via third-party technology
How to prevent	• Train people to be cautious of unexpected updates, tools, or third-party access requests • Vet vendors before use or integration • Monitor system access from third-party tools and services • Isolate third-party systems from critical infrastructure • Establish verification processes for high-risk supplier activity
How to contain	• Stop interacting • Alert security • Disable or disconnect affected third-party tools or integrations • Potentially isolate affected devices
How to remediate	• Reset passwords and revoke sessions • Scan affected devices for malware • Patch affected systems • Investigate vendor compromise • Monitor network for lateral movement and other suspicious activity
Cohorts most at risk	Developers; IT admins



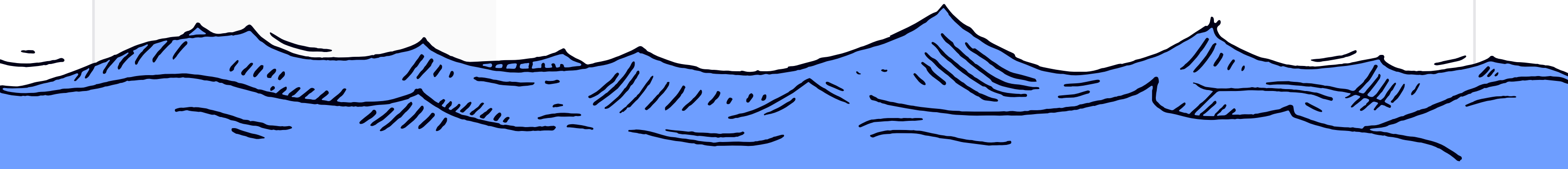
Callback phishing/tech support scam

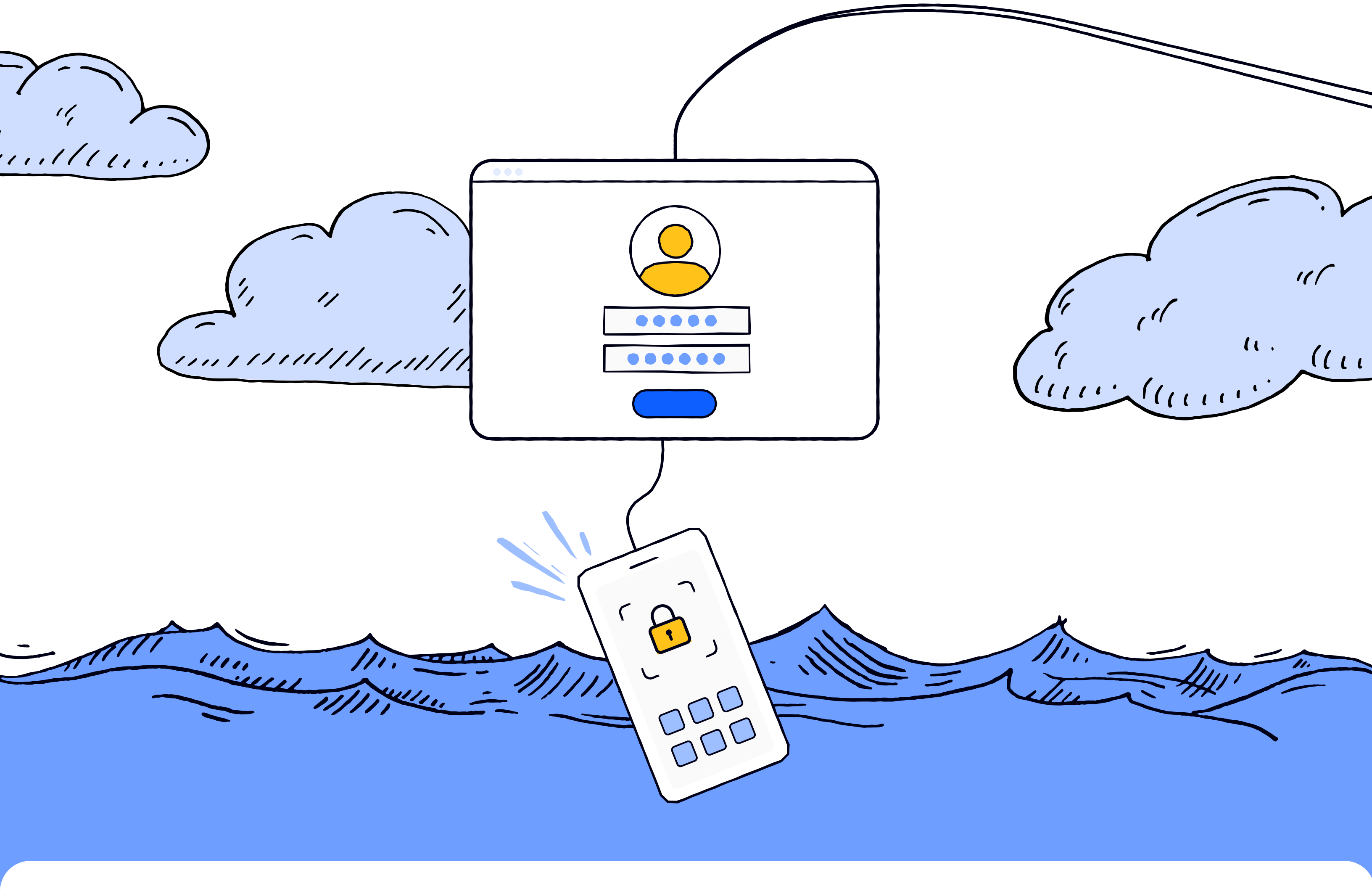
Delivery method	Email, followed by phone call
Description	Spoofed emails (often with a fake invoice attached)—impersonating an IT or tech support person—that trick victims into calling a fraudulent number and giving system access or installing malware.
How to prevent	• Train people to be cautious of unexpected voicemails or calls urging immediate action • Scrub personal and org chart data from data brokers and public sources • Block known scam numbers • Restrict remote access tools • Establish verification processes for granting remote access or making system changes
How to contain	• End call or don’t return call • Alert security • Capture recording of voicemail or call details • Potentially isolate devices if people affected
How to remediate	• Reset passwords and revoke sessions • Scan device for malware • Monitor network for lateral movement and other suspicious activity
Cohorts most at risk	Everyone



Lateral phishing

Delivery method	Internal email or messaging app
Description	Messages from compromised internal accounts that trick victims into clicking malicious links or attachments.
How to prevent	• Train people to be cautious of suspicious internal messages, even from trusted coworkers, especially if they contain an urgent request to click on a link or download an attachment • Monitor internal email activity for anomalies
How to contain	• Stop interacting • Alert security • Save message or capture screenshots • Notify affected people • Potentially isolate affected devices • Implement robust email security that monitors internal emails
How to remediate	• Reset passwords and revoke sessions • Scan affected devices for malware • Monitor network for lateral movement and other suspicious activity
Cohorts most at risk	Everyone





Reel it in: how Fable protects your people and organization

Social engineering isn't just a nuisance; it's one of the most effective, scalable ways attackers take advantage of people and breach organizations. The best defense isn't just awareness; it's action. This guide has armed you with the knowledge to recognize, respond to, and recover from today's most common (and costly) tactics.

Fable Security helps you stay ahead of these threats by delivering real-time, targeted interventions when and where they're needed most. We don't rely on generic training. We shape behavior in the moment, reducing risk across your organization without bogging people down.

The best strategy in dealing with social engineering attacks is to ward them off before they happen. With Fable, you can understand your organization's true human risk, prioritize the riskiest behaviors, and take targeted action—right when and where it matters most.

Don't take the bait.
Get Fable.
See a demo today.

Get a demo

Your guide to modern social engineering "ishes" and how to prevent, contain, and remediate them.