ACXIOM IPG

Cybersecurity in the Contemporary Workspace

What Do You Need to Know

Release date: December 2025

Cyber Trends

- ✓ Hype from new innovations overshadowing known and emerging threats
- ✓ Adversaries not investing in new attack vectors
- ✓ Low cost tried and true methods continue to reap rewards for bad actors

Weak Authentication

Supply Chain Attacks

Code Defects

Social Engineering

Check Washing

Fraudulent Web Sites

Cloud Platform Misconfigurations

Phishing Attacks

Orphaned Dial Up Modems

Vulnerability Exploits

IPG ACXIOM

Phishing Attacks / Business Email Compromise

IPG ACXIOM

What is a Phishing Attack?

- Phishing is a malicious scam devised to steal user data such as login credentials and is one of the most common means of online scams.
- Smishing, phishing attack over text messaging
- Vishing, phishing attack over voice

Phishing Attack Awareness Tips

Remember these three key Don’ts:

1. Don’t Click on That Link – Before you triple check the authenticity
2. Don’t Trust Unsecure Sites – Ensure the URL of the website starts with HTTPS
3. Don’t Disclose Personal Information – Never enter personal information on suspected sites

Learn to Identify Phishing

- Urgency
- Money Baits
- Look for Grammar Mistakes
- Impersonal Messages

Don’t Fall into the False Sense of Security

- Be Aware of Spear Phishing
- Learn to recognize Targeting Phishing Tactics

Update Regularly

- Keep Your Software Up to Date
- Turn On Automatic Updates
- Always Update Your Browser

Business Email Compromise (BEC)

- A type of cybercrime where the scammer uses email to trick someone into sending money or divulging confidential company information
- There has been a significant rise in BEC attacks
- Incidents involved employees being tricked into providing credentials, leading to unauthorized access to email accounts

What to do?

- Question emails that…
  - Are not from a known sender
  - Seem odd/abnormal
  - Create urgency/confusion
  - The receiver feels coerced

What To Do if a Suspected BEC Is Received?

- Report suspicious activity to your Security or IT team
  - Receiving a large amount of spam emails
  - Hang up on any unexpected IT calls, especially if they don't recognize the person calling and never grant remote access without verification
- This type of attack preys on confusion and trust
- Vigilance and quick action are key to protecting people and systems

LoanDepot

JAN 2024

Suspected Phishing Attack	The attack is believed to have begun with ransomware infections spread through seemingly safe files that contained hidden malicious code. Alphv/BlackCat ransomware group claimed responsibility for the attack
17M Customers affected	Data included, names, addresses, financial account numbers, social security numbers (SSNs), phone numbers, and dates of birth (DoB). The cyberattack left LoanDepot's millions of customers unable to make payments or access their online accounts for weeks.

The cost of incident and ransom not disclosed

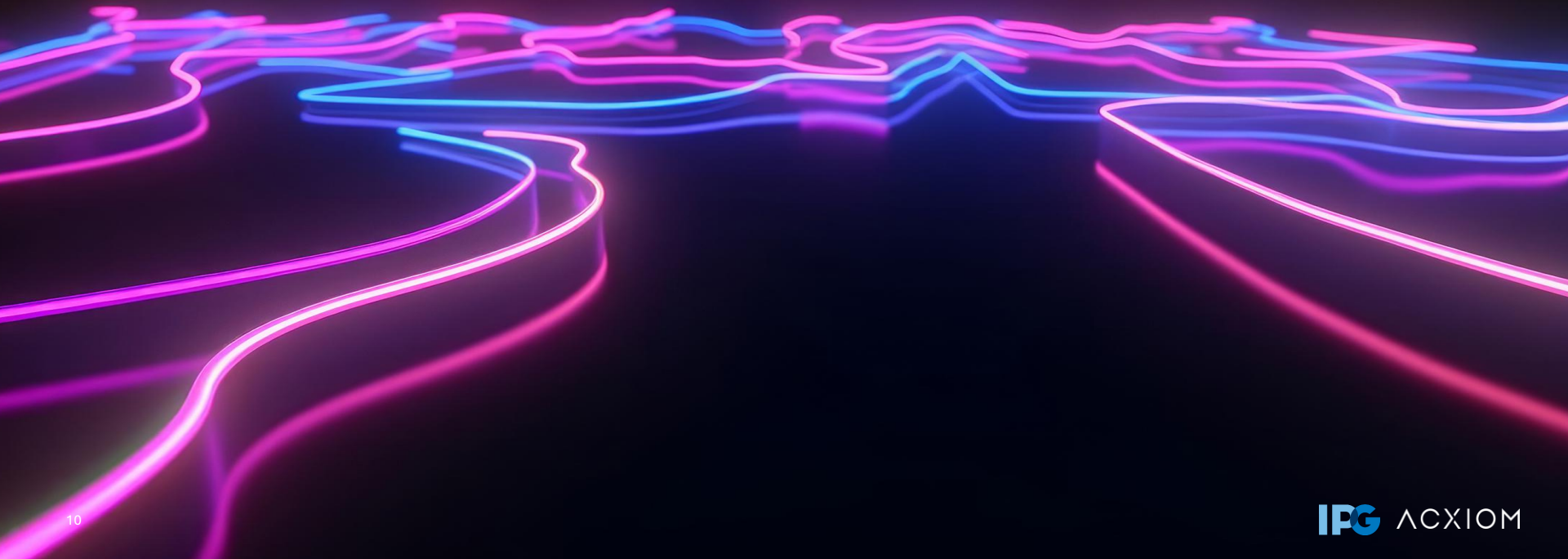
Arup

Feb 2024

Vishing Attack	Arup, a United Kingdom-based engineering firm, confirmed it fell victim to one of the most audacious deepfake scams ever seen.
$25.6M Paid	An employee in the organization's Hong Kong office was tricked into transferring a staggering $25 million to fraudsters after participating in a video conference call where everyone else, including senior executives, was an artificial intelligence (AI)-generated fake.

The cost of incident and ransom not disclosed

Social Engineering



What is Social Engineering?

The manipulation of people into performing actions or divulging confidential information by exploiting human psychology rather than technical hacking. Attackers use deceptive tactics like phishing, creating urgency, or impersonating authority figures to gain trust and trick individuals into compromising security systems, revealing passwords, or downloading malware. Google

How Social Engineering Works

Psychological Manipulation: Attackers exploit emotions and innate human traits, such as curiosity, helpfulness, fear, and greed, to trick victims

Impersonation: Attackers may pretend to be trusted individuals or organizations, like IT support or a company executive, to seem legitimate

Creating Urgency: They often create a sense of urgency to prevent the victim from thinking critically, such as by claiming a security threat or a pending financial loss

Exploiting Trust: They leverage trust, either pre-existing or by appearing as a trusted source, to gain access to sensitive information or systems

Google

Metro Goldwyn Meyers (MGM)

SEP 2023

Social Engineering	• Scattered Spider members researched MGM employees on LinkedIn, gathering information about their roles and identities • Using the gathered information, the attackers chose an MGM employee to impersonate • The hackers called MGM's IT help desk, posing as the employee and successfully convinced the help desk into providing them with login credentials • Using the obtained credentials, Scattered Spider gained administrator privileges to MGM's Okta and Azure tenant environments • The attackers used their high-level access to move laterally within MGM's systems
Effects of Attack, 13 Days	• Gambling operations were disrupted as slot machines went offline with displayed error messages • Hotel guests complained that their digital room keys stopped working • Online reservation and booking systems were shut down • Mobile services were interrupted as the MGM app became completely inaccessible • Email systems were affected • Restaurant reservations were disrupted

IPG ACXIOM

Prudential Financial

FEB 2024

Social Engineering	A noted Alphv affiliate tracked as Scattered Spider, Octo Tempest and UNC3944 has, used effective social engineering techniques thanks to its members' ability to speak American English Spanish Police Bust Alleged Leader of Scattered Spider
2.5M Customers affected	The compromised data included names, addresses, driver's license numbers, and non-driver identification card numbers

The cost of incident and ransom not disclosed

Weak Authentication

What is Weak Authentication?

An insufficient security mechanism that fails to adequately verify a user's identity, making systems vulnerable to unauthorized access. It often involves relying on a single, easily compromised factor like a weak password, or a process that has logical flaws or other vulnerabilities that can be exploited.

Google

Identity is the new perimeter

Characteristics of Weak Authentication

Single-factor authentication: Relying on just one credential, such as a password, is a common form of weak authentication.

Vulnerable to attacks: Passwords can be guessed, stolen through phishing, or brute-forced, allowing attackers to gain access.

Dependent factors: When multiple authentication factors are used but are dependent on each other, the compromise of one can lead to the compromise of others.

Broken authentication: This refers to security vulnerabilities in the authentication implementation itself, such as logic flaws or poor coding, which an attacker can bypass entirely.

Google

Change Healthcare

APR 2024

Weak Authentication	Lack of adequate remote access authentication. Specifically, it was found that multi-factor authentication (MFA) controls were absent on an application that allowed staff to remotely access systems.
$22M in Ransom paid to Alphv/BlackCat	Once inside the system, the cybercriminals did not immediately launch their attack. Instead, they loitered within the network for nine days. This allowed them to navigate through the network, identify valuable data, and strategize their next moves without raising alarms.

Remember all those movies about machines coming alive and attacking?
Well about that…

It’s not what you think

What is a Supply Chain Attack?

A supply chain attack is a cyber-attack that seeks to damage an organization by targeting less-secure elements in the supply chain... (Wikipedia)

WHAT IS OLD, IS NEW AGAIN

"In order to disrupt the Soviet gas supply, its hard currency earnings from the West, and the internal Russian economy, the pipeline software that was to run the pumps, turbines and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds”

The blast occurred in the summer of 1982. "The result was the most monumental non-nuclear explosion and fire ever seen from space”

Thomas C. Reed, a former Air Force secretary, At the Abyss: An Insider's History of the Cold War

Supply Chain Events

OCT & DEC 2023

Okta, OCT 2023
Stolen Credentials

- Scope, support case management system
- Data in scope of the incident, (i.e., username, full name, email address, etc.)
- Password not in scope, multifactor authentication in place
- Identity services not affected
- Risk, information is used for spear phishing attacks
- The cost of incident not disclosed

MongoDB, DEC 2023
Phishing Attack

- Scope, corporate applications used to provide support services to MongoDB customers
- Data in scope, (i.e., username, full name, email address, etc.)
- Password not in scope, multifactor authentication in place
- Clusters containing data not affected
- Risk, information is used for spear phishing attacks
- The cost of incident not disclosed

Supply Chain Events

JUN 2024

Snowflake
Weak Authentication

- Attack vector, password stuffing using credentials bought on the Dark Web
  - Multifactor authentication (MFA) for user accounts and network restrictions for services accounts was not in place
  - 165 Snowflake customers affected
- What has changed to allow this attack?
  - Traditionally, databases were the last tier of a multi-tiered architecture with no Internet access
  - Now, accessible directly from the Internet through consoles and API's
  - Companies and vendors have not adapted to identities being the new perimeter
- The cost of incident not disclosed

Table Stakes, How to Mitigate Supply Chain Attacks

- Stay informed with threat Intelligence feeds that alert you new threats
- Quarantine and scan open-source software
- Have an effective third-party risk management program that evolves with the everchanging risks and threats
  - Review application providers' software development lifecycle and secure coding practices
  - Review providers that software development is not within the direct-line-of-sight of their line of business, (e.g., HVAC, CCTV, vending machines, and anyone who wants to plug into your network)
- Require cyber liability insurance from providers
- Segment the internal network to limit access to critical areas
- Restrict Internet access from critical network zones and vendor supplied solutions
- Increase internal network monitoring
- An aggressive patching program that can quickly react to new threats
- Up to date incident response plan and prepare messaging for client, partner, and press inquiries

Cyber Tips

- Think Before you Download Apps
  - Just because you don’t use the software or app you installed doesn’t mean that it’s not using your device. Delete unused software/apps to increase the device’s available space and reduce your attack surface.
- Be Diligent
  - Be diligent about privacy and security settings, including who can access your documents and devices. Take a few minutes to configure these settings before using new devices or accounts and periodically revisit them to address any changes needed.
- When Appropriate, Turn on Auto-Updates
  - Any device that connects to the internet is vulnerable to risks. If you connect it, protect it. The best defense is to keep your device’s software, browser and operating system up to date.
- Keep Your Devices LOCKED
  - Set your devices to automatically lock when they’re not in use.
- Don’t Scan Unknown QR-CODES
  - Never scan a QR-CODE from an unknown source, they can be used to steal your personal data or direct you to a malicious site that could exploit your mobile.

Cyber Tips, Continued

- Danger-Danger with Public Wi-Fi
  - Keep wi-fi off when you don't need it. When on, the wi-fi hardware in your computer is still transmitting data between any network within range. Even though there are security measures in place to prevent this compromise, not all wireless routers are the same and hackers are smart!
- Don't Be an Easy Target
  - Be careful not only what you post online but what you read and believe. As AI becomes more advanced, the risk that it will be used for nefarious purposes becomes much greater.

No single tip is foolproof but practicing them in parallel is the best way to maintain good online hygiene, protect yourself, as well as the people and networks with whom you connect, from cyberattacks.


IPG ACXIOM