

Research Project on Phishing Attack Incident that led to sensitive information being exposed.





INCIDENT OVERVIEW: THE CRELAN BANK PHISHING ATTACK

DATE: 2016

TYPE OF ATTACK: WHALING (A HIGHLY TARGETED PHISHING ATTACK)

TARGET: CRELAN BANK (BELGIUM)

METHOD:





CYBERCRIMINALS USED **BUSINESS EMAIL COMPROMISE (BEC)** TACTICS, IMPERSONATING A SENIOR EXECUTIVE—LIKELY THE CEO—TO INSTRUCT AN EMPLOYEE (TYPICALLY IN THE FINANCE DEPARTMENT) TO PERFORM A CONFIDENTIAL AND URGENT WIRE TRANSFER.

ATTACK CHARACTERISTICS:

1. HIGHLY PERSONALIZED AND WELL-RESEARCHED.
2. EXPLOITED INTERNAL TRUST IN AUTHORITY FIGURES.
3. DID NOT RELY ON MALWARE—JUST SOCIAL ENGINEERING.



Impact Assessment

Category	Description
 Financial Loss	Approximately €70 million was stolen.
 Reputational Damage	Loss of client confidence and increased scrutiny in the financial sector.
 Operational Disruption	Required internal audits and system/process overhauls.
 Regulatory Implications	Prompted discussions on accountability and security standards in banking.

🔧 RESPONSE AND MITIGATION MEASURES

CRELAN BANK RESPONDED WITH IMMEDIATE AND LONG-TERM ACTIONS:

- A. **INTERNAL AUDIT:** FULL REVIEW OF INTERNAL COMMUNICATION AND FUND TRANSFER PROCESSES.
- B. **REPORTING:** INFORMED LAW ENFORCEMENT AND COOPERATED WITH REGULATORS.
- C. **PROCESS LOCKDOWN:** HALTED ALL SIMILAR TRANSACTIONS AND REQUIRED EXTRA VERIFICATION.
- D. **STAFF TRAINING:** DEPLOYED AWARENESS CAMPAIGNS ON PHISHING AND SOCIAL ENGINEERING.
- E. **POLICY REVISIONS:** INTRODUCED STRICTER APPROVAL WORKFLOWS FOR SENSITIVE FINANCIAL OPERATIONS



Technical Safeguards

- A. **Email Authentication Protocols:** Use Of SPF, DKIM, And DMARC To Verify Email Legitimacy.
- B. **Multi-factor Authentication (MFA):** Required For All Sensitive Operations And System Access.
- C. **Ai-based Email Filtering:** Detect And Block Suspicious Or Spoofed Emails.
- D. **Endpoint Detection And Response (EDR):** Monitor And Respond To Unusual Device Behavior.



Organizational Policies

- A. **Dual Authorization:** Require Two Separate Approvals For High-value Transfers.
- B. **Clear Escalation Paths:** Employees Must Have Defined Procedures To Escalate Suspicious Instructions.
- C. **Strict Role-based Access:** Ensure Only The Right People Have Access To Financial Systems.



Human Factor – Training & Culture

- A. **Regular Phishing Simulations:** Test Employee Awareness With Mock Phishing Attempts.
- B. **Mandatory Cybersecurity Training:** Focused On Email Threats, CEO Fraud, And Social Engineering.
- C. **Promote Security Culture:** Encourage To Question Irregular Requests especially From Senior Staff.



HOW CRELAN BANK (AND OTHERS) CAN PREVENT FUTURE ATTACKS

Crelan's prevention strategy going forward should focus on:



1. **Zero Trust Framework:** Trust no one by default—verify everything.
2. **Behavioral Analytics:** Identify anomalies in communication and transaction patterns.
3. **Cybersecurity Governance:** Have an active security board that reviews risks quarterly.
4. **Incident Response Drills:** Practice scenarios regularly to ensure preparedness.
5. **Industry Collaboration:** Share threat intelligence with other banks via ISACs or FS-ISAC.

SONY PICTURES ENTERTAINMENT HACK

IN NOVEMBER 2014, SONY PICTURES ENTERTAINMENT (SPE) WAS THE VICTIM OF A MASSIVE CYBERATTACK BY A GROUP CALLING ITSELF “GUARDIANS OF PEACE” (GOP). THE ATTACKERS INFILTRATED SONY’S NETWORK, STOLE AND LEAKED CONFIDENTIAL DATA, AND DEPLOYED DESTRUCTIVE MALWARE THAT WIPED COMPANY SYSTEMS.

KEY ELEMENTS OF THE ATTACK:

RELEASE OF INTERNAL EMAILS, FINANCIAL RECORDS, UNRELEASED FILMS, AND PERSONAL EMPLOYEE INFORMATION.

USE OF A MALWARE CALLED “**DESTOVER**”, WHICH RENDERED MANY OF SONY'S COMPUTERS INOPERABLE.

THREATS OF TERRORIST ATTACKS RELATED TO THE RELEASE OF *"THE INTERVIEW"*, A COMEDY FILM MOCKING NORTH KOREA’S LEADER KIM JONG-UN.

CULPRIT:

THE FBI ATTRIBUTED THE ATTACK TO **NORTH KOREA**, MARKING IT AS A CASE OF STATE-SPONSORED CYBER WARFARE.

IMPACT ASSESSMENT

1. FINANCIAL IMPACT

A. ESTIMATED COST: OVER **\$100 MILLION**.

B. DISRUPTION TO OPERATIONS, INCLUDING LOSS OF EMPLOYEE PRODUCTIVITY, RESTORATION COSTS, AND LEGAL LIABILITIES.

2. OPERATIONAL IMPACT

A SYSTEMS WERE SHUT DOWN FOR WEEKS.

B MASSIVE DISRUPTION TO INTERNAL COMMUNICATIONS AND WORKFLOWS.

3. REPUTATIONAL DAMAGE

EMBARRASSMENT DUE TO LEAKED EMAILS (E.G., RACIALLY INSENSITIVE COMMENTS BY EXECUTIVES).
DAMAGED RELATIONSHIPS WITH PARTNERS, TALENT, AND EMPLOYEES.

4. LEGAL AND HR ISSUES

LAWSUITS FROM EMPLOYEES DUE TO PERSONAL DATA EXPOSURE.
HEIGHTENED SCRUTINY OVER CYBERSECURITY AND HR PRACTICES.

Sony Pictures Hack (2014)

A high-profile cyberattack linked to North Korea, resulting in a massive data leak and demonstrating the intersection of cybersecurity with international geopolitics.

Response and Mitigation

1. IMMEDIATE ACTIONS TAKEN

SONY TOOK ITS SYSTEMS OFFLINE AND BEGAN INCIDENT RESPONSE PROCEDURES.
ENGAGED CYBERSECURITY FIRMS LIKE MANDIANT FOR FORENSICS AND RECOVERY.
WORKED WITH THE **FBI, DHS**, AND OTHER FEDERAL AGENCIES.
PUBLICLY CANCELED AND LATER DIGITALLY RELEASED *"THE INTERVIEW"* TO DEFY THREATS.

2. TECHNICAL MITIGATION

REBUILT IT INFRASTRUCTURE AND NETWORKS FROM SCRATCH.
ENHANCED ENDPOINT PROTECTION AND MALWARE DETECTION SYSTEMS.
INSTITUTED BETTER DATA ENCRYPTION AND ACCESS CONTROLS.

3. COMMUNICATION

SONY'S LEADERSHIP COMMUNICATED WITH STAKEHOLDERS AND THE PUBLIC UNDER PRESSURE.
MANAGED CRISIS PR AROUND THE LEAKED MATERIALS.

RECOMMENDATIONS & FUTURE PREVENTION

A. CYBERSECURITY RECOMMENDATIONS

1. SEGMENTATION OF NETWORKS TO ISOLATE CRITICAL SYSTEMS.
2. REGULAR PENETRATION TESTING AND VULNERABILITY ASSESSMENTS.
3. 24/7 SECURITY OPERATIONS CENTER (SOC) MONITORING.
4. USE OF ZERO TRUST ARCHITECTURE TO MINIMIZE LATERAL MOVEMENT OF ATTACKERS.

B. EMPLOYEE TRAINING

1. REGULAR PHISHING SIMULATIONS AND SECURITY AWARENESS PROGRAMS.
2. CLEARLY DEFINED INCIDENT RESPONSE POLICIES AND DRILLS.

C. INCIDENT RESPONSE PLAN (IRP)

1. UPDATED TO INCLUDE DETAILED PLAYBOOKS FOR RANSOMWARE AND NATION-STATE ATTACKS.
2. COORDINATION WITH LAW ENFORCEMENT BUILT INTO THE IRP.

HOW SONY OVERCAME IT

A. RECOVERY STRATEGY

1. SONY REBUILT ITS NETWORK INFRASTRUCTURE ALMOST ENTIRELY.
2. SIGNIFICANT INVESTMENT IN CYBERSECURITY TECHNOLOGIES AND POLICIES.
3. RESUMED NORMAL OPERATIONS WITHIN MONTHS DESPITE INITIAL CHAOS.



B. REPUTATION MANAGEMENT

1. ISSUED PUBLIC APOLOGIES FOR LEAKED CONTENT.
2. IMPROVED TRANSPARENCY AND INTERNAL POLICIES.
3. SLOWLY REGAINED TRUST AMONG EMPLOYEES AND STAKEHOLDERS.

C. LESSONS LEARNED

1. BECAME A CASE STUDY IN THE IMPORTANCE OF CYBERSECURITY AT THE BOARD LEVEL.
2. THE HACK SERVED AS A WAKE-UP CALL FOR THE ENTERTAINMENT INDUSTRY AND BEYOND.



The Sony Pictures hack of 2014 was a watershed moment in cybersecurity history, demonstrating how cyberattacks can impact corporate operations, finances, and reputation. Through a combination of technical overhaul, improved policies, and strong public relations management, Sony was able to recover and emerge more resilient. The incident led to widespread changes across industries in how organizations approach cybersecurity threats — especially those from state-sponsored actors.

CYBERATTACK DISRUPTS POWER TO HUNDREDS OF THOUSANDS IN UKRAINE

1. Overview

What happened:

On **December 23, 2015**, a sophisticated cyberattack targeted **three regional electricity distribution companies** in Ukraine: **Kyivoblenergo, Prykarpattiaoblenergo, and Chernivtsioblenergo**.

Key Features of the Attack:

- Attackers remotely took control of SCADA (Supervisory Control and Data Acquisition) systems.
- They **switched off circuit breakers**, cutting power to about **230,000 people** for several hours.
- Simultaneously launched a **telephony DoS (TDoS)** attack on customer service lines.
- Used **BlackEnergy 3 malware** to gain access, followed by **KillDisk** to wipe data and make recovery harder.



Culprit:

- Widely attributed to the **Russian state-sponsored group "Sandworm"**, although not officially confirmed by Russia.

2. Impact Assessment

A. Infrastructure Disruption

- **230,000 people** lost power in the middle of winter for 1 to 6 hours.
- Manual operations had to be initiated due to system failure.
- Permanent damage to some network components and IT infrastructure.

B. Technological Impact

- The use of **KillDisk malware** wiped critical data, delaying restoration.
- Attackers used **firmware corruption** techniques on serial-to-ethernet devices, disabling remote restoration.

C. Psychological & Geopolitical Impact

- Demonstrated how cyberattacks could target **critical infrastructure**.
- Increased public fear and international attention.
- Set a precedent for hybrid warfare involving cyber tactics.

3. Response and Mitigation

A. Immediate Response

- Manual override of electrical substations by on-site personnel.
- Isolated infected systems to prevent further spread.
- Used **paper-based processes and analog systems** where possible.

B. Technical Response

- Full rebuild and reinstallation of SCADA systems.
- Investigated the malware and intrusion paths with help from international cybersecurity experts (e.g., ESET, SANS ICS).

C. Government Coordination

- Ukraine's **CERT-UA** collaborated with international partners, including the **U.S. Department of Homeland Security (DHS)**.



4. Recommendations and Future Prevention

A. Cybersecurity Upgrades

- Hardened SCADA environments (air-gapped or segmented networks).
- Disabled remote access for critical infrastructure.
- Introduced **multi-factor authentication (MFA)** and **role-based access**.

B. Monitoring and Detection

- Implemented **Intrusion Detection Systems (IDS)** on industrial control networks.
- Continuous **network behavior monitoring** for anomalies.

C. Training and Awareness

- Regular cybersecurity drills for power company staff.
- Better coordination between IT and operational technology (OT) teams.

D. Incident Response Planning

- Developed formal **incident response and recovery playbooks**.
- Established **national-level coordination centers** for critical infrastructure protection.

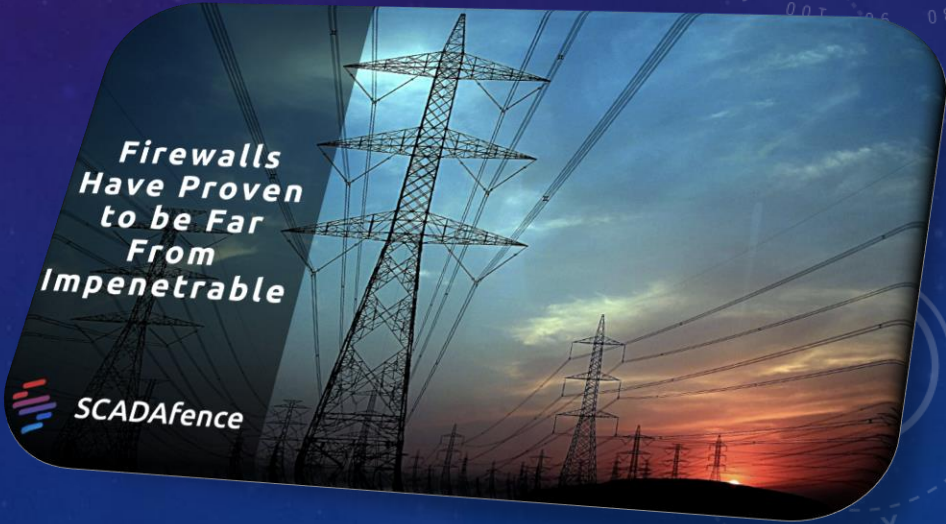
How Ukraine Overcame It

Infrastructure Resilience

- Manual controls and trained technicians allowed power to be restored within hours.
- Avoided long-term outages thanks to operational preparedness.

International Support

- Received aid and threat intelligence from NATO, EU partners, and cybersecurity firms.
- Became a global model for cooperation on critical infrastructure cyber defense.



Cyber Defense Modernization

- Ukraine significantly modernized its **cyber command**, including the creation of specialized cyber units.
- Implemented strict cybersecurity requirements for all critical infrastructure operators.

Prepared for Future Attacks

- Despite a second, more sophisticated attack in 2016, Ukraine responded faster and contained it better.
- By 2022, Ukraine demonstrated **high cyber resilience** during the Russian invasion, leveraging lessons learned from 2015.

The 2015 Ukrainian Power Grid Attack was a groundbreaking incident in cyberwarfare history, revealing the vulnerabilities of critical infrastructure. Ukraine's quick manual response, international collaboration, and long-term strategic reforms helped the nation not only recover but also emerge as a leader in cyber defense preparedness. The incident pushed global critical infrastructure sectors to reassess and strengthen their cybersecurity posture.

FACC AG BUSINESS EMAIL COMPROMISE (BEC) SCAM

Incident Overview

- In January 2016, FACC fell victim to a Business Email Compromise (BEC) scam, specifically a "whaling" attack. Attackers impersonated CEO Walter Stephan, sending a fraudulent email to the finance department requesting a substantial fund transfer for a supposed acquisition project. The email was meticulously crafted, mimicking the CEO's communication style to avoid suspicion. Consequently, the finance department transferred approximately €50 million to accounts controlled by the fraudsters .

Impact Assessment

- **Financial Loss:** FACC suffered a direct financial loss of around €50 million.
- **Operational Disruption:** The incident led to significant internal upheaval, including the dismissal of CEO Walter Stephan and the CFO .
- **Reputational Damage:** The breach eroded stakeholder trust and highlighted deficiencies in the company's internal controls.
- **Regulatory Scrutiny:** The attack attracted attention from regulatory bodies, prompting reviews of FACC's compliance and security protocols.

Response and Mitigation

Following the attack, FACC undertook several measures:

- **Leadership Changes:** The company dismissed its CEO and CFO to address accountability and restore confidence .
- **Policy Revisions:** FACC reviewed and strengthened its internal processes, particularly those related to financial transactions and executive communications.
- **Employee Training:** The company emphasized cybersecurity awareness, educating staff on recognizing and responding to phishing attempts.

Recommendations

To prevent future whaling or BEC attacks, companies should adopt the following:

People

- **Executive Training:** C-level executives should receive cybersecurity awareness training specifically on whaling attacks.
- **Company-Wide Awareness:** Regular phishing simulations and real-case reviews.

Processes

- **Dual Authorization:** Require multiple sign-offs for large financial transfers or sensitive requests.
- **Callback Verification:** Independently confirm high-risk email requests by phone or video—especially those from executives.

Technology

- **Email Security Tools:** Use SPF, DKIM, and DMARC to prevent spoofed emails.
- **AI Email Filtering:** Detect unusual behavior and language patterns in communications.
- **Access Controls & Logging:** Restrict who can authorize transactions and audit trails for traceability.

Future Preventions

Long-term cybersecurity resilience depends on:

Cultural Shift

- **Security-First Mindset:** Encourage questioning of unusual instructions, regardless of source.
- **Blame-Free Reporting:** Encourage staff to report suspicious emails or mistakes early, without fear of punishment.

Governance and Policy

- **Crisis Playbooks:** Maintain incident response plans with roles, escalation paths, and recovery steps.
- **Board-Level Cyber Oversight:** Cyber risk must be a standing agenda item at executive and board meetings.

External Collaboration

- **Join ISACs (Information Sharing & Analysis Centers):** Share threat intelligence with industry peers.
- **Cyber Insurance:** Transfer part of the financial risk via insurance, while ensuring coverage for social engineering.

The FACC whaling attack was preventable. It succeeded due to a **lack of awareness, poor internal controls, and unquestioned authority**. Companies that **overcome** such attacks are the ones that:

- Learn from failure
- Strengthen internal governance
- Empower employees to challenge instructions
- Use technology and policies to verify, not just trust



HILLARY CLINTON CAMPAIGN EMAIL LEAK

1. Incident Overview

What Happened:

- In 2016, during the U.S. presidential election campaign, emails from the Democratic National Committee (DNC) and Hillary Clinton's campaign chairman, **John Podesta**, were **illegally accessed and leaked**.
- The leaks were carried out by Russian state-sponsored hackers, allegedly under the aliases "**Fancy Bear**" and "**Cozy Bear**", linked to **GRU**, Russia's military intelligence agency.
- The contents were published by platforms like **WikiLeaks**, just months before the election.

Methods Used:

- **Phishing attacks** were the primary vector. John Podesta was tricked into clicking a malicious link that allowed attackers to gain access to his Gmail account.
- Attackers exploited weak cybersecurity practices and lack of two-factor authentication (2FA).

Timeline Highlights:

- **March 2016:** Podesta's Gmail account was compromised.
- **June-July 2016:** DNC emails were leaked to WikiLeaks.
- **October 2016:** WikiLeaks began releasing Podesta's emails, with daily dumps throughout the month.

2. Impact Assessment

Political Impact:

- The leaks were damaging to Hillary Clinton's campaign, creating internal conflict and negative media cycles.
- Emails showed favoritism towards Clinton over Bernie Sanders, contributing to division within the Democratic Party.
- Fueled conspiracy theories and political polarization.

Cybersecurity Impact:

- Highlighted the vulnerability of major political entities to state-sponsored cyberattacks.
- Raised public awareness about phishing and email security threats.

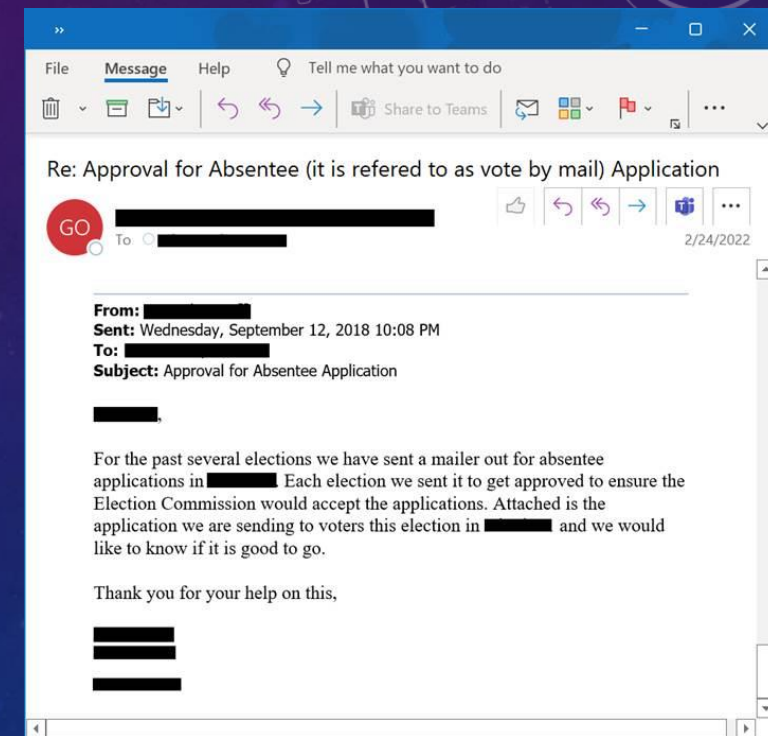
Legal and Intelligence Impact:

- Triggered multiple investigations, including by the FBI and Special Counsel Robert Mueller.
- Led to indictments of **12 Russian intelligence officers** in 2018.

3. Response and Mitigation

Immediate Actions:

- The Clinton campaign and DNC acknowledged the leaks but questioned their authenticity and motives.
- Security firms like **CrowdStrike** were brought in to analyze and confirm the breach.
- The U.S. intelligence community publicly attributed the attacks to Russian state actors.



Long-Term Responses:

- Cybersecurity overhauls within the DNC and other political organizations.
- Federal efforts to secure electoral infrastructure and political campaigns.
- Improved coordination between private tech companies and the U.S. government to counter disinformation.

4. Recommendations and Future Preventions

Technical Measures:

- **Mandatory Two-Factor Authentication (2FA)** for all campaign and staff accounts.
- **Regular phishing awareness training** for all staff members.
- Use of **secure email platforms**, like ProtonMail or G Suite with advanced protections.
- Continuous **security audits and penetration testing**.

Organizational Policies:

- Establish a **chief information security officer (CISO)** or dedicated cybersecurity lead for all major campaigns.
- Create and rehearse **incident response plans** specific to cyberattacks and data leaks.



Governmental and Legislative Actions:

- Pass stronger **cybersecurity standards for political parties**.
- Expand funding and support from **CISA (Cybersecurity and Infrastructure Security Agency)** for campaign security.
- Improve international norms and accountability mechanisms for **state-sponsored cyberattacks**.

Public Awareness and Media Literacy:

- Educate the public on how to identify manipulated or out-of-context information from leaks.
- Promote **fact-checking platforms** and partnerships with social media to combat disinformation.



Summary: Hillary Clinton Campaign Email Leak (2016)

In 2016, during the U.S. presidential election, Russian state-sponsored hackers infiltrated email systems belonging to the Democratic National Committee (DNC) and Hillary Clinton's campaign chairman, **John Podesta**. The attackers used **phishing emails** to gain access, most notably tricking Podesta into giving up his Gmail credentials.

Thousands of emails were subsequently leaked to **WikiLeaks**, causing widespread controversy. The leaks revealed internal campaign strategies and tensions within the Democratic Party, contributing to political polarization and harming Clinton's campaign.

The U.S. intelligence community later attributed the attack to **Russian military intelligence (GRU)**. This incident highlighted the vulnerabilities in political cybersecurity and played a significant role in shaping U.S. cyber defense policy.