5 AI-Enhanced Cyber Attacks That Could Impact Credit Departments

By: Chris Woodard, CMO & Co-Founder, Handle.com

Originally published in the Credit Research Foundation's publication, Perspective by CRF (Q3 2024)

Today, financial risks involve more than unpaid bills—they also include AI-powered cybersecurity threats.

Cybercriminals are now using advanced AI to carry out cyberattacks, posing a serious threat to financial systems and the security of sensitive data. AI enables cybercriminals to execute attacks with incredible speed, scale, and automation. It's crucial for credit professionals to stay informed about these evolving threats and to take necessary precautions. Just as credit policies are robust, cybersecurity measures must be equally strong to safeguard financial data and operational integrity.

With cyber threats evolving, all employees, not just IT specialists, need to take a proactive stance in addressing this issue.

Here are five cyberattacks amplified by AI, which credit professionals must be particularly vigilant about. Learn the practical steps to fortify your organization against these potential threats.

1. Sophisticated Phishing Attacks

What is Phishing?

Phishing is a type of cyberattack where attackers attempt to deceive you into divulging sensitive information like login credentials or financial data, often by masquerading as a trustworthy entity. AI has elevated phishing by enabling attackers to craft highly convincing and personalized messages using natural language processing and machine learning.

How It Can Happen in Your Office

You receive an email that looks like it's from a trusted client or a high-level executive within your company. The email might ask you to update payment information or authorize a transaction.

With AI, these phishing emails can be tailored to reference specific details about your recent transactions or client interactions, making them look authentic. If your team members fall for these convincing scams, it could lead to unauthorized transactions or data breaches.

This scenario played out recently at Framework, a San Francisco-based tech company. An employee at their external accounting partner, Keating Consulting, fell victim to a phishing attack. The attacker, posing as the CEO, requested sensitive customer data. The accountant provided a spreadsheet containing personal information and outstanding balances, which could now be used to impersonate the company and commit fraud.

What You Can Do:

- **Use Advanced Email Filtering:** Implement AI-based email security solutions to detect and block fraudulent messages before they reach your inbox.
- **Conduct Regular Training:** Educate your team on identifying phishing attempts and verifying suspicious requests.
- **Establish Verification Procedures:** Always confirm sensitive requests through secure channels, like direct phone calls or encrypted messaging systems.

2. Advanced Ransomware

What is Ransomware?

Ransomware is malicious software that locks victims out of their systems or encrypts files, demanding a ransom payment to restore access. AI-enhanced ransomware can spread more quickly and adapt to evade detection by traditional security measures.

How It Can Happen in Your Office

Imagine an employee downloads an attachment from an email that appears to come from a known sender. Once the attachment is opened, ransomware activates and encrypts critical financial documents and client data. The malware could spread across your network, disrupting operations and potentially corrupting vital financial records.

Consider the recent incident involving Allan McNeill Chartered Accountants, a well-established firm specializing in agribusiness services. On August 19, 2024, the firm suffered a ransomware attack orchestrated by a group known as RansomHub. The attackers exploited vulnerabilities in the firm's cybersecurity defenses to exfiltrate approximately 30GB of sensitive data. This data, potentially including confidential financial information, was then held for ransom.

What You Can Do:

- **Regularly Back Up Data:** Ensure backups are conducted frequently and stored in a secure location separate from your main systems.
- **Deploy AI-Powered Threat Detection:** Check that your office uses advanced security solutions that swiftly detect and take action against ransomware threats as they arise.
- **Educate Employees:** Train staff on safe practices, such as avoiding suspicious attachments and links and recognizing potential ransomware signs.

3. Intelligent Credential Stuffing

What is Credential Stuffing?

Credential stuffing is an attack where cybercriminals use lists of stolen or leaked usernames and passwords to gain unauthorized access to accounts. AI enhances this attack by automating the process, allowing attackers to test large numbers of credentials rapidly and efficiently.

How It Can Happen in Your Office

Cybercriminals could obtain stolen credentials from data breaches and use AI to automate login attempts on your company's financial systems or client portals. If successful, they could gain access to sensitive financial data or internal systems, leading to potential fraud or unauthorized transactions.

Cisco recently warned about the notable increase in brute-force attacks targeting VPN services and web application authentication interfaces. Attackers used automated tools to test large volumes of stolen credentials against these services.

This trend highlights how AI-driven credential stuffing can exploit vulnerabilities in login systems. For example, if your company uses a VPN or web-based financial management tool, attackers could exploit compromised credentials to gain unauthorized access, potentially accessing sensitive financial data and disrupting operations.

What You Can Do:

- **Implement Multi-Factor Authentication (MFA):** Add an extra security layer requiring users to provide verification beyond just a password.
- **Enforce Strong Password Policies:** Mandate using complex, unique passwords and regular changes.
- **Monitor Login Activity:** Use AI-based tools to detect and block suspicious login attempts and unusual access patterns.

4. Adaptive Malware

What is Adaptive Malware?

Adaptive malware is malicious software that uses AI to modify its behavior to evade detection by security systems. This malware type can dynamically change tactics to avoid traditional defenses and remain undetected.

How It Can Happen in Your Office

Adaptive malware could infiltrate your network through infected email attachments, malicious links, or compromised software. Once inside, it might alter its behavior to avoid detection by antivirus programs, corrupting financial records, or intercepting communications. Its ability to adapt makes it particularly challenging to identify and remove.

Adaptive malware can wreak havoc by targeting the accounting systems used in your organization. For instance, consider a scenario where malware is introduced through a phishing email disguised as a routine payment request. Once installed, this malware can monitor and manipulate online payment transactions in real time. It might intercept payment instructions, alter amounts, or redirect funds to unauthorized accounts without raising immediate alarms. It's essential to ensure that your vendors comply with cybersecurity standards.

A recent incident of this type of attack involved sophisticated banking malware that operates by overlaying legitimate mobile banking apps with fake screens. Users, believing they are interacting with their genuine banking application, inadvertently provide their login credentials and One-Time Passwords (OTPs) to the malware. This same technique could be adapted to target platforms credit professionals use, allowing attackers to capture payment details or manipulate transactions.

What You Can Do:

- **Adopt Advanced Endpoint Detection:** Utilize AI-based endpoint protection to identify and respond to unusual behaviors or activities on your network.
- **Regularly Update Security Software:** Keep your antivirus and anti-malware solutions up-to-date to protect against evolving threats.
- **Segment Your Network:** Isolate critical systems and sensitive data to limit malware's potential spread and impact.

5. AI-Enhanced Social Engineering

What is Social Engineering?

Social engineering is a manipulation technique used by attackers to deceive individuals into divulging confidential information or compromising security by exploiting human behavior rather than technical vulnerabilities.

AI enhances these attacks by creating highly realistic fake personas and orchestrating sophisticated scams.

How It Can Happen in Your Office

Thanks to AI voice cloning technology, you might receive a phone call from someone who sounds exactly like a trusted executive. This impersonator could request urgent changes to financial transactions or seek sensitive information. The realistic nature of the voice and detailed knowledge about your business can make the request seem credible, leading to potential financial losses or unauthorized disclosures.

The Town of Plymouth recently fell victim to a social engineering scam involving fraudulent invoices. Scammers first breached a vendor's system, gaining access to project information, and then used this information to send fake invoices to the town's Finance Department. These invoices appeared legitimate and contained incorrect payment instructions. Due to insufficient verification procedures, the Finance Department processed payments totaling $104,150 to the scammers.

In your office, similar tactics could be used to deceive your accounts payable team into paying fraudulent invoices or transferring funds to unauthorized accounts. For instance, scammers might impersonate a known supplier or business partner by emailing altered payment details. Without verifying these changes through a secure channel, your organization could suffer significant financial losses.

What You Can Do:

- **Implement Strict Verification Procedures:** Always verify requests involving business-critical information through official and secure channels.
- **Use Voice Authentication:** Employ technologies that verify the authenticity of voice communications.
- **Update Training:** Regularly train employees to recognize social engineering tactics and verify requests through proper channels.

Strengthening Your Cybersecurity Posture

AI-driven cyberattacks are a growing threat to credit professionals and their organizations. As these technologies evolve, so do the tactics of cybercriminals. Credit professionals must adopt a proactive approach to cybersecurity to protect sensitive financial data and ensure operational integrity.

Cybersecurity is a shared responsibility that goes beyond the IT department. By incorporating advanced security measures, implementing strong verification procedures, and continually educating employees, you can reduce the risks posed by AI-enhanced threats. Staying informed and vigilant is essential to protect your company's financial assets and maintain trust with clients and partners. Embrace a comprehensive security strategy to make sure that your company can withstand sophisticated cyberattacks and effectively handle the complexities of modern threats.

About the Author

Chris Woodard is the CMO and Co-Founder of Handle.com. Handle's software powers the largest credit and finance teams in construction. Fortune 500 material suppliers and contractors trust Handle on a daily basis to provide their credit and collections departments with an end-to-end solution that saves their staff 10-12 hours per week.