Cybersecurity 101: Common Types of Cyberattacks

By John Sanche, Peter Ciechanowski, Mardi McNaughton and Lily Yao

In today's digital world, cybersecurity is no longer just an IT issue; it is a business imperative. From ransomware attacks to phishing scams, cyber threats are growing in scale and sophistication. They affect organizations of all sizes and across all industries and the consequences can be financially and operationally devastating.

Understanding the Most Common Types of Cyberattacks

Understanding the types of cyber breaches is the first step toward building a strong defence. Below provides a high-level overview of seven of the most prevalent forms of attack that businesses should be aware of.

1. Malware: The Multi-tool of Cybercrime

Malware, short for malicious software, is a broad category of malicious software designed to infiltrate systems, steal data, and/or disrupt operations.[1] It comes in many forms, including ransomware, spyware, viruses, worms, and trojans, and can be tailored to suit the attacker's goals. What makes malware especially dangerous is its adaptability. Especially now, with the help of AI, attackers can more effectively disguise malware within deepfake[2] websites or emails that look real, making it harder for users to spot and avoid.[3] These tools allow malware to slip past traditional defences and cause damage before being detected.

2. Phishing: Deception at Scale

Phishing attacks use fake communications, including emails, texts, QR codes, or even Wi-Fi networks, to trick individuals into revealing sensitive information or downloading malware. A highly-publicized example of such an attack was the 2020 phishing attack on Twitter employees via their phones. In that case, hackers successfully gained access to high-profile accounts, including those of Bill Gates, Kim Kardashian, and Joe Biden, and enabled them to post a fraudulent bitcoin scam that generated over $100,000 USD. This shows how a single lapse in employee judgment can lead to widespread corporate consequences. Phishers are also using AI to make their messaging more personalized and sophisticated. Since ChatGPT's release in late 2022, there has been a 4,151% increase in malicious phishing emails globally.[4] The prominence of AI is making it more difficult to distinguish legitimate messages from fraudulent ones, making it even more important to verify information and its source.

3. DoS and DDoS Attacks: Flooding the Gates

Denial-of-Service (**DoS**) and Distributed Denial-of-Service (**DDoS**) attacks aim to overwhelm a system with traffic, rendering it inaccessible to users. While DoS attacks originate from a single source, DDoS attacks are coordinated across thousands of compromised devices, making them harder to block. These attacks can cripple websites and disrupt services thereby causing financial losses, particularly for companies that rely heavily on their websites being accessible. AI has made these attacks more precise and scalable, allowing attackers to identify weak points and time their strikes for maximum impact. For certain businesses, even a short disruption can lead to lost revenue and damaged reputation.

---

[1] Malware can infiltrate a system through deceptive links, infected attachments, or software vulnerabilities that allow it to install without the user's knowledge.
[2] Deepfakes are fake but realistic-looking digital content including images, videos, or websites, created using artificial intelligence. They can mimic real people or trusted brands, tricking users into thinking they are legitimate.
[3] Canada introduced Bill C-63, known as the *Online Harms Act*, which is the first federal legislation to explicitly address deepfakes. It aims to combat the spread of harmful online content, including non-consensual deepfake pornography and fraudulent uses of deepfake technology.
[4] See the new report, "**The State of Phishing: 2024 Mid-Year Assessment**" by cybersecurity firm SlashNext.

4. Man-in-the-Middle Attacks: The Invisible Eavesdropper

In a Man-in-the-Middle (**MiM**) attack, a hacker secretly intercepts communication between two parties, for example a customer and a bank, without either party knowing. Communications are intercepted when attackers hijack Wi-Fi connections or insert themselves between two parties to secretly monitor or alter data in transit. The attacker can steal login credentials, financial data, or other sensitive information, often by redirecting users to fake websites or injecting malicious code into legitimate communications. These attacks are especially dangerous in business environments where secure data exchange is routine. AI tools now help attackers automate the process of identifying vulnerable connections and executing MiM attacks with minimal detection.

5. SQL Injection: Exploiting Web Application Weaknesses

Structured Query Language (**SQL**) injection involves an attacker inserting malicious code into a website's input fields (like login forms) to manipulate its database. Attackers insert malicious code by entering specially crafted text into website forms that do not properly check inputs. This tricks the system into running harmful database commands. Afterwards, attackers can access, modify, or delete sensitive data from within the victim's system. Proper input validation and secure coding practices are essential to prevent these attacks.

6. Zero-Day Exploits: Attacks with No Warning

Zero-day exploits occur when attackers discover and use a software vulnerability before the vendor is aware of it, meaning there is no patch or fix available at the time of the attack. These exploits are particularly dangerous because they strike without warning and often go undetected until after damage is done. For instance, in 2022, hackers exploited an undiscovered flaw in Google Chrome to infect users' devices via fake job offer emails. These emails contained links to counterfeit job search sites like Indeed and ZipRecruiter. When targets clicked on these malicious links, their browsers were automatically infected with malware.

7. DNS Tunneling: Hiding in Plain Sight

Domain Name System (**DNS**) tunneling involves an attacker hiding malicious data inside normal internet traffic, allowing attackers to bypass firewalls and exfiltrate data undetected. Because DNS traffic is rarely scrutinized, this method is particularly stealthy. Detecting and mitigating DNS tunneling requires advanced monitoring tools and a legal strategy for managing potential data breaches.

By understanding the types of cyberattacks and the legal landscape surrounding them, businesses can better protect themselves and their stakeholders. For more information, contact any member of our **Privacy and data protection group**.