# How Hackers Get Company Data

Recently, corporate giants Microsoft, Samsung and Okta revealed that hackers breached their systems. While high-profile attacks like these make global news, SMBs silently fall prey to hackers daily. But when companies understand how hackers get company data, they can strengthen their defenses.

Undeniably, cyber criminals grow more sophisticated every day. They run their hacking operations like corporations and constantly improve their tools and techniques. Too often, however, organizations simply leave the door wide open for bad actors. Unpatched software, weak passwords and a lack of security awareness offer an open invitation to attack.

## Unpatched Software Leaves Vulnerabilities

Hackers constantly look for vulnerabilities in software programs. Responsible vendors release security updates with critical patches before hackers can exploit them. However, those patches only protect organizations that install the updates in time.

## Weak Passwords Fall to Brute Force Attacks

Another common hacking method involves brute force attacks. In these attacks, hackers use automated tools to try and guess passwords. While the process can prove time-consuming, weak passwords make it much easier. Then, with access to a single account, bad actors take the first step toward entering the network and accessing sensitive data.

## Malware Opens the Door

Malware refers to a family of malicious software programs designed to infect systems. In many cases, victims unwittingly download malware by clicking an email attachment or accessing an infected website. Once the malware downloads, hackers can use it to record usernames and passwords, install spyware or ransomware and generally create havoc.

## Old-fashioned Observation Yields Clues

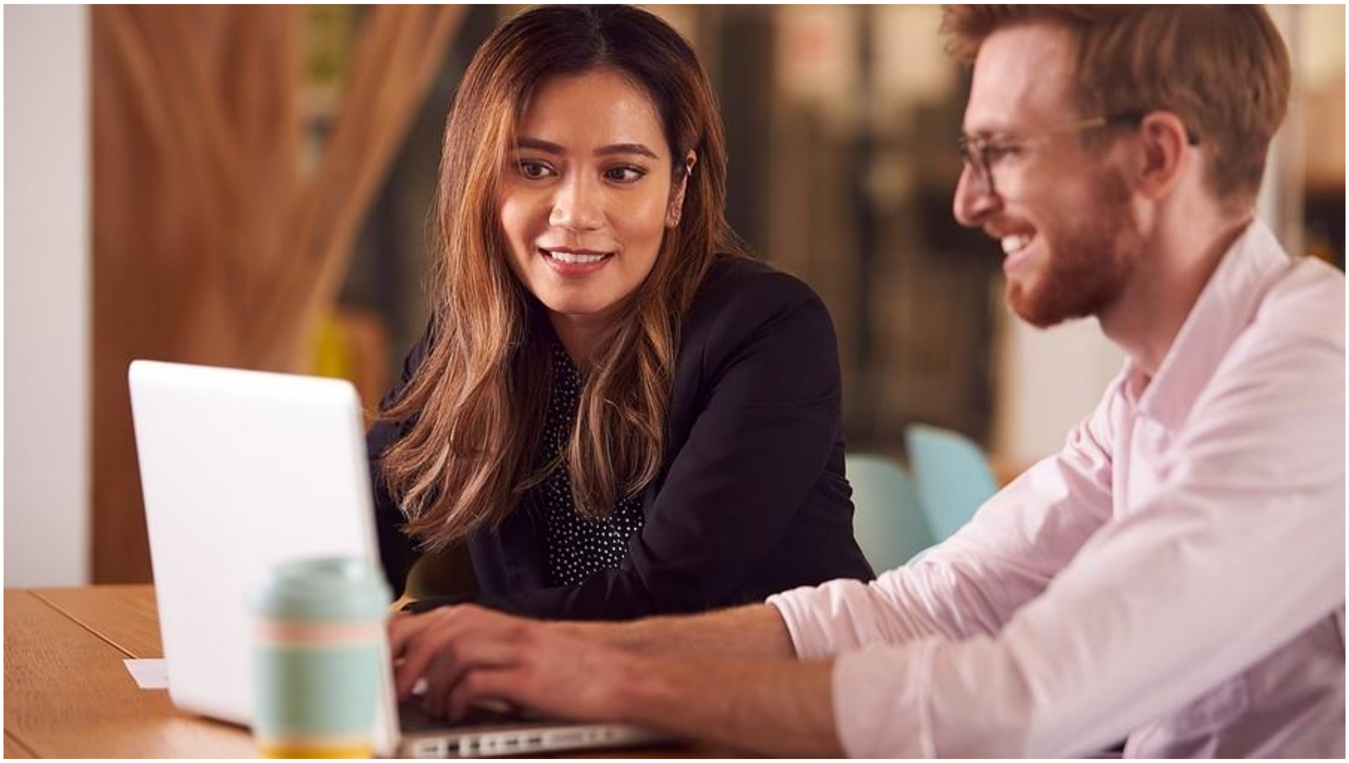
Sometimes, the first step into a victim's system involves simple observation. For instance, with the rise of remote work, coffee shops provide a popular spot for a change of office scenery. But employees do not always use care when accessing sensitive information in a public setting. The person at the neighboring table can learn a lot with a quick click of a phone camera.

Likewise, social media offers a treasure trove of information for bad actors looking to build a victim profile. A savvy hacker can learn a great deal about a company from a few LinkedIn searches, the company website and a scroll through Facebook posts and Twitter feeds. Using that information, they can quickly build a successful phishing campaign.

## Phishing Attacks for the Win

With all the advancements in hacking technology, phishing campaigns still account for a significant portion of effective cyber-attacks. In a phishing attack the bad guys impersonate a trusted executive or company and use that trust to trick victims into surrendering valuable information like credentials or company secrets.

Most often, the phishing attacks come through email. For example, an employee may receive an email message supposedly from a trusted company. The email indicates an alarming problem with their account and instructs the employee to click a fake link and then enter their login credentials.



## Hackers Get Company Data…But Only If You Let Them

The vast majority of data breaches result from human error, such as when an employee falls for a phishing email. This means that many breaches can be prevented when companies use cybersecurity best practices.

Regular security awareness training goes a long way, for example. Additionally, companies should install software patches quickly, implement email filters and encryption and strengthen password policies.

No single security strategy will block all hackers. However, the email and cybersecurity experts at Messaging Architects can help organizations build a layered cybersecurity strategy, beginning with email filters. We can help you configure security controls precisely to match your work environment and protect vital digital assets.