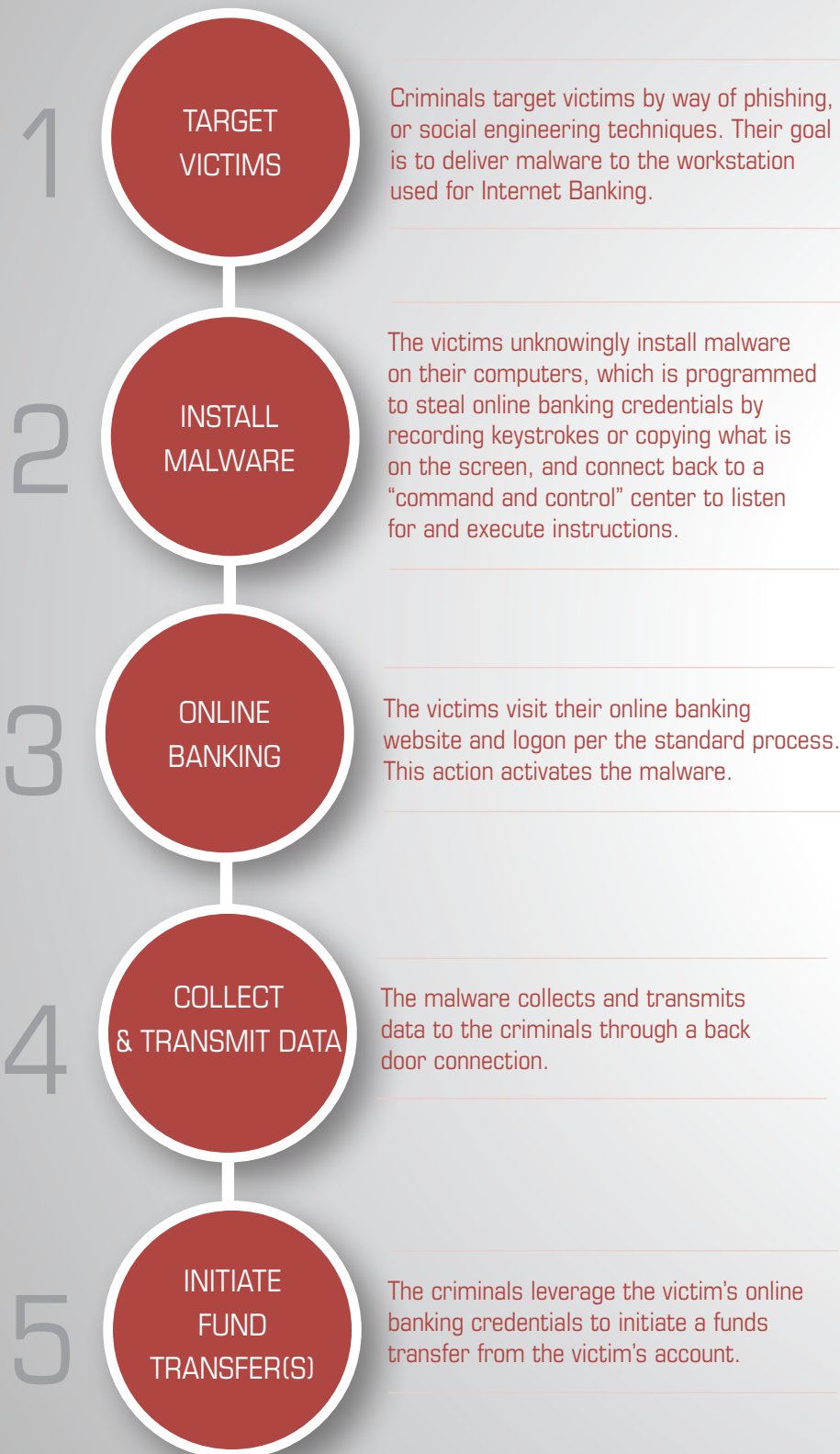


# WHAT IS A CORPORATE ACCOUNT TAKEOVER?

Well-organized cybercrime syndicates are targeting small and medium size business, municipalities, non-profits and school districts across the country. Cyber criminals use **malicious software** (known as **malware**) in order to steal a business' online banking credentials or take over web sessions. They then attempt to steal thousands, even hundreds of thousands of dollars, by creating fraudulent ACH or wire transfers. This crime is known as Corporate Account Takeover.

It is very important to recognize that Corporate Account Takeover attacks are not aimed at financial institutions; they target accountholders, specifically the computers and Internet connections that are used to access online bank accounts. It is the accountholder's responsibility to secure workstations, network connections and account credentials. Federal Regulation E does not apply to commercial accounts and financial institutions are not required to reimburse losses under certain circumstances.

## Anatomy of a Corporate Account Takeover



## ...and how to prevent it.



**Monitor and reconcile your account.** Reviewing accounts regularly helps enable quick detection of unauthorized activity, and allows your business and your financial institution to take action to prevent or minimize losses.

**If you suspect a compromise...** Immediately disconnect your workstation from the internet, cease all online banking activity on all workstations and call your financial institution.