What is Phishing and Pharming

Pharming

Pharming uses computer software, such as crimeware, malware or spyware, to collect personal information from your computer and deliver it back to fraudsters. In pharming, consumers who are attempting to log onto a legitimate Web site are unknowingly redirected by the fraudulent software to an authentic-looking but bogus site. When the consumer enters his or her personal log-in information, the criminals capture this sensitive information and may use it for a variety of violations, including accessing your accounts and making online purchases. Since little or no participation on your part is necessary, and the redirect happens behind the scenes, pharming is extremely difficult to detect.

Phishing

Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Many phishing scams come through emails with warnings such as "IMPORTANT: Account Verification" or "Unauthorized Account Access". Sites such as PayPal and other popular purchase sites are hijacked and these counterfeit websites are used to steal your information. Social-engineering schemes use these 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Hijacking brand names of credit unions, banks, e-retailers and credit card companies, phishers often convince recipients to respond. Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning.