

Welcome to the Gemini IBD® Cybersecurity Infographics Newsletter Phishing Trends in 2022

12TH EDITION, VOLUME 1
FEBRUARY 16, 2022

There is no doubt that 2021 was one of the most challenging for Cybersecurity. Many new threat variants evolved, but most notably, it was the year for Ransomware attacks, especially the Supply Chain ones. It is expected that 2022 will be the same or even worse, with a changing geopolitical climate being yet another powerful catalyst. But, Phishing will still continue to be the dominant threat vector.

What Is Phishing and Who Is Doing It?

Phishing is a type of social engineering attack in which malicious actors send legitimate-looking emails to trick people into revealing their personal or financial information. The key difference between phishing and many other forms of cyber-attacks is that phishers have a seemingly legitimate reason for requesting your information.

The Types of Phishing Attacks To Be Aware Of

There are some common phishing attacks that many of us have heard of which can include ransomware, malware, and good-old-fashioned viruses. However, phishing needs to be looked at as a category on its own. Plus, under phishing, there are variants that people need to understand, such as spear-phishing, whaling, vishing, and smishing.

How To Protect Yourself From Phishing

If you're not a cybersecurity expert or someone who has been trained on how to defend against social engineering attacks like phishing emails, then it's important to understand what steps you can take to minimize your risk. The three most critical things that will help protect you are:

- 1) Training
- 2) Prevention
- 3) Recognition and Response

The Most Targeted Victims

As with all other forms of online attacks, Phishing usually starts by targeting higher-value targets. Large corporations are juicy targets because they contain more email accounts than any other organization type in your country. Universities aren't behind on that regard either because students usually have access to their own email accounts as well as those of their friends who study in another university. Generally speaking, enterprises will have almost everything automated (e.g., automatic emails going out) and don't employ enough people to stay up on all security issues. The reality is that Phishing attacks are more of a problem for small-to-medium businesses than large corporations or universities because their employees are often less educated about internet safety.

In terms of industry, these are the most common targets:

- Healthcare Providers
- Financial Service Providers
- Extremely Busy Businesses

10 H A C K E D 100