Title A: How Phishing May Threaten Unsuspecting Users in 2019

Subtitle A: Learn about the latest phishing statistics affecting users.

Title B: Why Phishing Is a Bigger Threat Than Ever in 2019

Subtitle B: The latest phishing statistics show a clear trend.

Title C: How Phishing Threatens Unwary Users: 2019 Edition

Subtitle C: Phishing tactics are evolving to leverage new vulnerabilities.

https://pixabay.com/illustrations/hacker-hacking-cyber-security-hack-1944688/

In the world of cybersecurity, it's a well-known fact that 93% of data breaches trace their original attack vectors back to phishing. In the overwhelming majority of cases, hackers use phishing to get their foot in the door of the network they're targeting.

Phishing is not new, nor are many of the broad strategies that cybercriminals use when phishing.

However, the amount of data publicly available in today's Internet environment brings a new level of tactical sophistication to the arena.

This is immediately apparent when surveying some of the highest profile cyber attacks in 2019. The wealth of public data available on almost anyone makes it easy for cybercriminals to conduct highly targeted phishing attacks. Additionally, the newfound ability to automate this information gathering allows bad actors to expand their operations with ease.

What We Can Learn From the Biggest Data Breaches in 2019

A quick survey of some of the biggest data breaches so far in 2019 shows that cybercriminals are getting bolder and more capable as time goes on. A veritable underground economy of black hat hackers, phishing specialists, and service providers are cooperating with an unprecedented degree of sophistication.

1. DiscountMugs.com

In the first week of January, DiscountMugs.com announced that it was successfully targeted by a professional hacking group called Magecart. The group gained access to the company's payment processor application and skimmed credit card information from customers for four months.

Unlike many other e-commerce data breaches, hackers managed to get away with users' full unencrypted credit card information – everything they would need to make illicit purchases using the victims' identities.

Magecart hackers are smart enough to know that using victims' information would tip their hand. Instead, they sell victims' credit card information anonymously on the dark web, effectively obscuring their tracks.

https://unsplash.com/photos/IuLgi9PWETU

2. BenefitMall

On January 7th, BenefitMall announced that it had been victimized by a data breach originating with a phishing attack that compromised an employee account. The payroll and HR service provider hasn't revealed exactly how many records were compromised. The breach made customer names, addresses, social security numbers, birthdates, and bank account information available to hackers.

This example illustrates how dangerous a single employee's mistake can be. Because BenefitMall is a payroll processor, hackers knew it was virtually guaranteed that sensitive customer data would be present in any employee's email inbox.

If the company had been less prepared, a single compromised email account could easily have led to the entire company being compromised. An ambitious cybercriminal could take control of an executive account or pilfer company funds before turning on BenefitMall's customers and partners.

3. Catawba Valley Medical Center

Approximately 20,000 patients of the Catawba Valley Medical Center in North Carolina have had their personal data exposed in a sophisticated cyber attack announced in February 2019. Hackers successfully phished three employee email accounts during the summer of 2018 and obtained the names, birthdates, social security numbers, and health records of the medical center's patients.

This attack illustrates one of the cybercriminal industries' highest priority targets – healthcare providers. Even providers who are compliant with HIPAA regulation can be targeted. In the case of the Catawba Valley Medical Center, the clinic had never been out of compliance with HIPAA regulation.

4. UConn Health

UConn Health recently announced that roughly 326,000 patient records were accessed by unauthorized parties at the end of 2018. The health system provider's email accounts were compromised by phishing attacks that leaked patient names, birthdates, social security numbers, and medical data.

Healthcare providers like UConn Health are obliged to notify the U.S. Department of Health and Human Services whenever a breach affecting more than 500 people takes place. In this case, the company announced the breach and immediately offered free identity theft protection services to the patients whose social security information was compromised.

https://pixabay.com/illustrations/first-aid-icon-set-doctor-bags-1146983/

5. St. Francis Health System

One of the largest healthcare-related data breaches of 2019 to date targeted electronic health records systems partnered with St. Francis Physicians Systems. Cybercriminals targeted health record systems with public-facing portals and phished employee email accounts to gain access to patient names, addresses, birthdates, insurance information, social security numbers, and medical data.

The attack compromised 32,178 individual patient records. The clinic announced the data breach in March 2019. In this case, cybercriminals only gained access to the accounts of patients who had previously received medical services from Milestone Family Medicine, a third-party partner of St. Francis Physician Systems.

This attack showcases how compromised email accounts can allow cybercriminals to move laterally

through organizations and their partners. Just like the high-profile Target hack of 2013, third-party partners often represent the easiest attack vector for cybercriminal phishing attempts.

Phishing Trends to Watch Out for in 2019

There is a clear pattern in 2019's biggest data breaches. Cybercriminals have placed relatively small organizations – especially in the field of healthcare and e-commerce – squarely in their sights. The more sensitive information an organization is likely to have access to, the greater its risk of being targeted.

This explains why healthcare organizations are currently the most common targets of email phishing attempts. The Department of Health and Human Services maintains a publicly available "Wall of Shame" describing the very latest data breaches in the healthcare sector.

However, smaller organizations in e-commerce and finance are also being targeted. There is a clear tendency towards targeting small to mid-sized businesses that rely on third-party professional services. These organizations represent the largest and most accessible surface area for cyber attack and often do not invest in multi-layered security solutions appropriate to the threat.

Sources:

https://enterprise.verizon.com/resources/reports/dbir/

https://www.identityforce.com/blog/2019-data-breaches

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

https://www.hipaajournal.com/st-francis-physicians-services-notifies-patients-of-milestone-family-medicine-data-breach/

https://www.modernhealthcare.com/article/20190226/NEWS/190229939/uconn-health-email-breach-compromises-data-from-326-000-patients

https://www.paubox.com/blog/catawba-valley-medical-center-suffers-hipaa-email-breach

https://people.carleton.edu/~carrolla/story.html