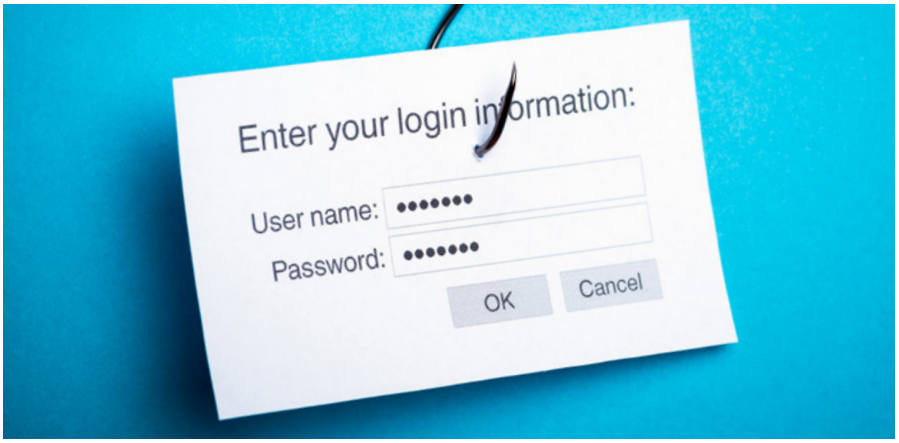
UHY LLP Certified Public Accountants

MANUFACTURING INSIDER

VOLUME 11 :: ISSUE 4

In This Issue:



PHISHING LESSONS

A pedestrian in New York sees a musician getting out of a cab and asks, "How do you get to Carnegie Hall?" The musician replies, "Practice, practice, practice!" It's an old adage but holds a lot of truth. To be good at any skill requires practice. How good are your employees at recognizing and managing phishing emails? It is a well-known fact that phishing emails are the number one cause of successful cyber-attacks. The statistics are compelling:

- 76% of businesses were victims of a phishing attack in 2018[i]
- 92% of malware is delivered by email[ii]
- 95% of attacks on business networks result from successful spear phishing[iii]
- The average cost of a phishing attack to a mid-sized company is $1.6 million[iv]
- 97% of people globally are unable to identify a sophisticated phishing email[v]
- 82% of manufacturers have experienced a phishing attack in the past year[vi]

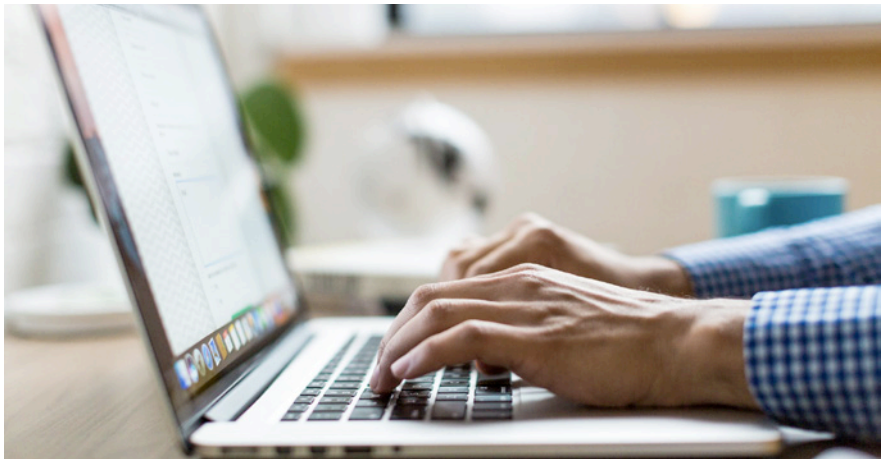
Clearly, phishing emails resulting in ransomware, data breaches and payment fraud are on the rise and targeting the middle market and sole proprietors at an ever-increasing rate. Most companies today are struggling to protect their businesses from these types of attacks. Middle market companies are particularly susceptible to cyber-attacks due to limited security personnel and budget for managing the ever-changing cybersecurity threat landscape. Many executives simply "don't know what they don't know" about cybersecurity and rely on a trusted employee or business partner to handle security along with all of the other information technology requirements of the business. For most IT resources at midsized companies, cybersecurity is at best a part-time endeavor. As a result, the limited IT resources cannot possibly stay ahead of the cyber-threat curve.

So, if phishing emails are the leading cause of cyber-attack, what is your organization doing to manage them? While there are many technology solutions on the market to identify and block phishing emails, the cold hard truth is that your best prevention is your "human firewall". There is nothing better at identifying and managing phishing threats than a well-trained employee. Your people are the ones receiving the phishing emails. They will be the ones that recognize them and handle them appropriately, or they will be the ones to open them and click on the link that leads to a cyber-attack in your organization.

Continued on Page 2...

The next level of service

Continued from Page 2...



Is your organization conducting phishing campaigns? If not, why not? In order for your employees to become proficient at recognizing and dealing with them properly, you must make them practice! Any parent that has paid for music lessons or coached a sports team knows the importance of practice. The skills required to effectively recognize and manage phishing emails are no different. They require practice.

It has been said that a cyber-attack on your organization is not a matter of "if," but "when." And chances are, it will be a phishing email that causes the attack. Let's face it, your employees are on the front lines of the war on phishing. They are your "human firewall". You owe it to them and to your company to give them the opportunity to practice their phishing recognition skills. Remember, it only takes one click by one employee on one phishing email to allow a cyber-attack which could result in significant financial and reputational damage to your company.

A properly developed phishing campaign can significantly improve the effectiveness of your "human firewall" and reduce the risk of a phishing related cyber-attack.We have seen first-hand the damaging effects of cyber-attacks. We have numerous clients who have been the victim of a ransomware attack which disabled their business for several days or weeks. We have clients who have been hit with wire-transfer and banking fraud resulting from Business Email Compromise (BEC). Each one was totally unprepared for a cyber event. Most had no cybersecurity training program and no active phishing campaigns.

Our firm first began to utilize active phishing campaigns in late 2016 as a result of our own struggles to deal with the flood of phishing emails and malware. Using a well-known phishing campaign tool, we ran our first phishing test unannounced to our entire employee base. Our results were typical. Thirty percent of our users clicked on embedded links in the test emails. Sixteen percent of our users supplied personal information on the linked phishing pages. Soon after our initial test, we provided mandatory awareness training for our entire staff. We went over the results of our initial campaign and thoroughly explained the impact. Our employees were surprised by the results of our initial test. Any one of those clicks could have resulted in malware or a data breach.

After our initial campaign, we continued to provide our employees with opportunities to practice recognizing phishing emails. We utilized the tools provided by our service provider and designed campaigns that were similar to the most prevalent and successful real-world phishing emails.

The results have been nothing short of amazing. Over the first year of our campaign, we noted a steady drop in the number of click-throughs by employees. In addition, our employees began reporting and avoiding more legitimate phishing emails! Our security staff continued to hone their phishing design skills to make it more challenging for our employees to spot the phishing tests. Over time, our risk rating for phishing-related cyber-attacks has gone from 30% to less than 3% as a result of the training and the regular practice in which our employees participate. That is a substantial reduction in risk! There is ample evidence that our results are not unique. A recent Ponemon Institute study found that training reduced click-throughs on phishing emails between 26% and 99%, with an average improvement of 64%.[vii]

It's all about practice. The better your employees are at recognizing a phishing email, the better chance your company will be able to avoid a costly and embarrassing cyber-attack. There is little doubt that a well-run phishing and training campaign will reduce the risk of a cyber-attack.

We have helped our clients design, deploy, and manage phishing campaigns that work. We can provide your people with the tools and training they need to become proficient in the battle against phishing scams. Contact a dedicated cybersecurity professional at UHY Advisors for more information on phishing campaigns and preparing your employees to minimize cyber risks.

By David Barton, Managing Director at UHY Advisors and a leader of the firm's Technology, Risk and Compliance practice. Barton specializes in information security and technology risk and controls

i https://www.wombatsecurity.com/state-of-the-phish
ii https://blog.alertlogic.com/must-know-phishing-statistics-2018/
iii https://www.explainhownow.com/2019/social-engineering/
iv https://blog.dashlane.com/phishing-statistics/
v ibid
vi https://www.phishingbox.com/news/phishing-news/check-point-research-2018-security-report-summary
vii Ponemon Institute: The Cost of Phishing & Value of Employee Training

CURRENT STATE OF THE MANUFACTURING INDUSTRY

According to a new Standard & Poor's report, there are two key indicators that will tell you what kind of shape the manufacturing industry is in. The first is the Institute for Supply Management's Purchasing Manager's Index and the second is the Federal Reserve's Capacity Utilization Index for motor vehicles and parts. A reading above 50 percent for the ISM index indicates that manufacturing is expanding in the US, and below 50 means that it is contracting. History shows that each time since 1983 that the index fell below 43 percent "speculative grade" automotive companies began to panic. Similarly any time the Fed's utilization rate dropped below 72 percent during that period, it caused stress to automotive companies. Let's take a look back at the trend over the past year:

RECENT TREND

AS OF **AUG '19**

ISM Purchasing Manager's Index: 49.1% 

Fed Capacity Utilization Rate: 75.7% 

AS OF **JUN '19**

ISM Purchasing Manager's Index: 51.7% 

Fed Capacity Utilization Rate: 78.1% 

AS OF **FEB '19**

ISM Purchasing Manager's Index: 55.3% 

Fed Capacity Utilization Rate: 75.4% 

AS OF **DEC '18**

ISM Purchasing Manager's Index: 54.1% 

Fed Capacity Utilization Rate: 75.7% 

MANUFACTURING INDUSTRY INSIGHT

UHY LLP recognizes that manufacturing companies require their auditors, tax specialists and business advisors to add value to financial reporting activities. That is why we combine the strength of business and financial expertise with a hands-on, "shop floor" approach to solving complex business decisions in these key segments:

- Aerospace & Defense
- Distribution
- Automotive Suppliers
- Industrial Manufacturing
- Consumer Products

Our professionals are leaders in the industry and take the steps necessary to ensure our client's future success by identifying and addressing new trends, accounting requirements and regulations.

OUR LOCATIONS

CA Irvine 949 623 8803
CT Farmington 860 676 9020
FL Miami 305 438 7993
GA Atlanta 678 602 4470
MD Columbia 410 423 4800
MI Ann Arbor 734 213 1040
MI Detroit 313 964 1040
MI Farmington Hills 248 355 1040
MI Sterling Heights 586 254 1040
MO Kansas City 816 741 7882
MO St. Louis 314 615 1301
NY Albany 518 449 3171
NY Long Island 631 712 6860
NY New York 212 381 4800
NY Saratoga Springs 518 583 1234
NY Rye Brook 914 697 4966
TX Houston 713 325 7870

NATIONAL OFFICES

MI Farmington Hills 248 522 3000