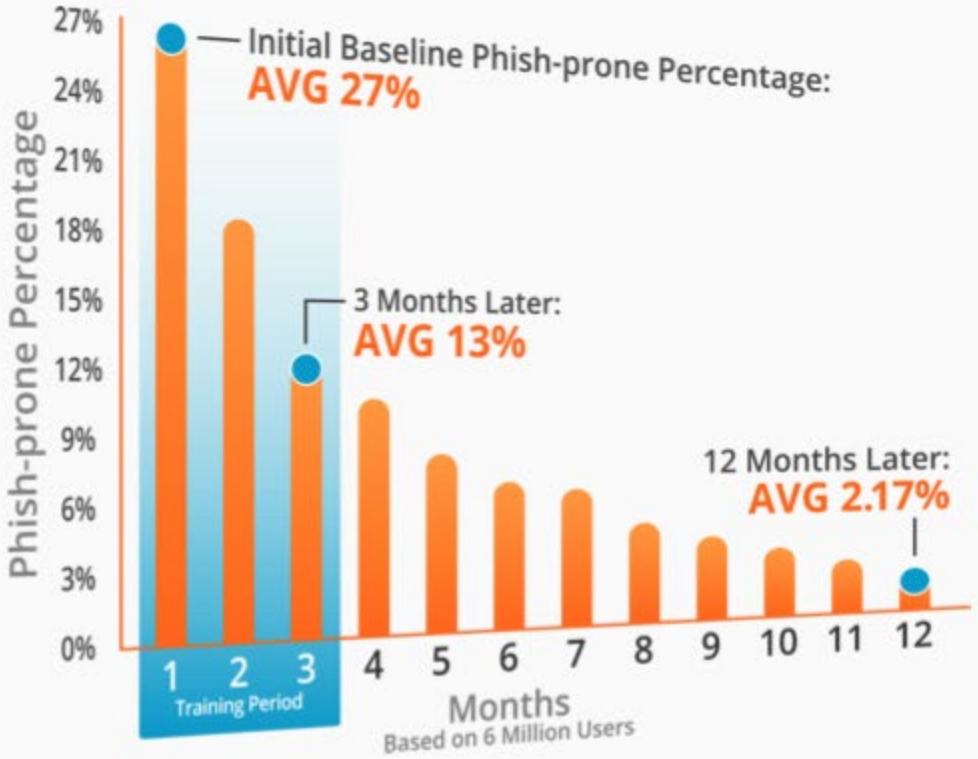
Security Awareness Training
How is it important to **you**?

KnowBe4
Human error. Conquered.

What is a phishing email?

A phish is an email that appears to be from reputable companies or someone known to you in order to get you to reveal personal information, such as passwords and credit card numbers. The personal information gathered can then be used for fraudulent or illegal purposes.

A Successful Security Awareness Program WORKS



People are a critical layer within the fabric of our Security Programs

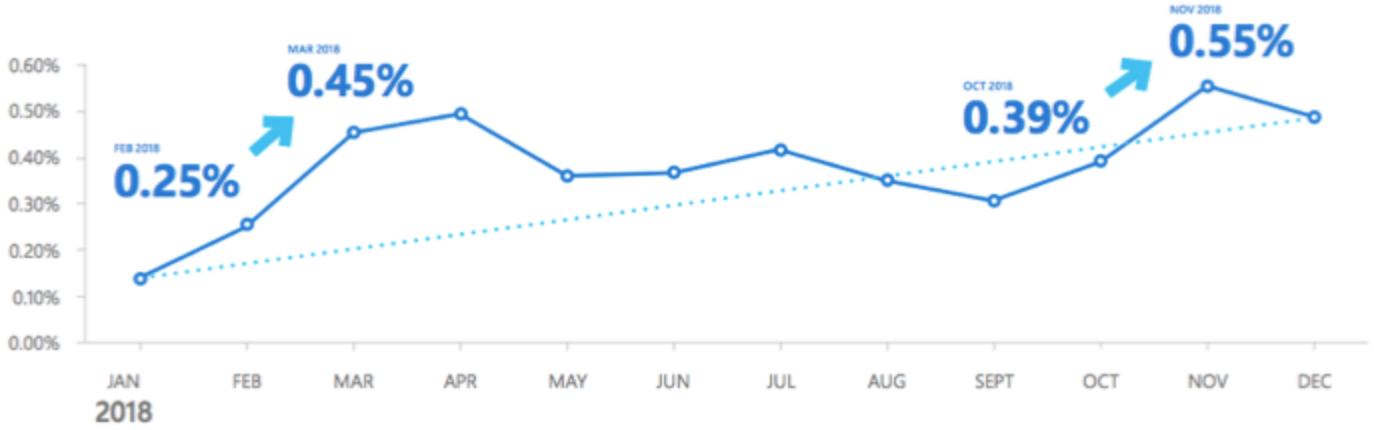
We are the 8th Layer in Security

i.e. Building the **HUMAN FIREWALL**

8. Security Awareness Layer
7. Application Layer
6. Presentation Layer
5. Session Layer
4. Transportation Layer
3. Network Layer
2. Datalink Layer
1. Physical Layer

Phishing Rates are Still on the Rise

Percentage of total inbound emails that are phishing emails



PHISHING CONTINUES TO BE A PREFERRED ATTACK VECTOR IN 2018

Microsoft analyzes and scans in Office 365 more than 470 billion email messages every month for phishing and malware, which provides analysts with considerable insight into attacker trends and techniques. The share of inbound emails that were phishing messages increased 250 percent between January and December 2018. Phishing remains one of the top attack vectors used to deliver malicious zero-day payloads to users, and Microsoft has continued to harden against these attacks with additional anti-phishing protection, detection, investigation, and response capabilities to help secure users.

▲ **FIGURE 8.**

Phishing emails in 2018

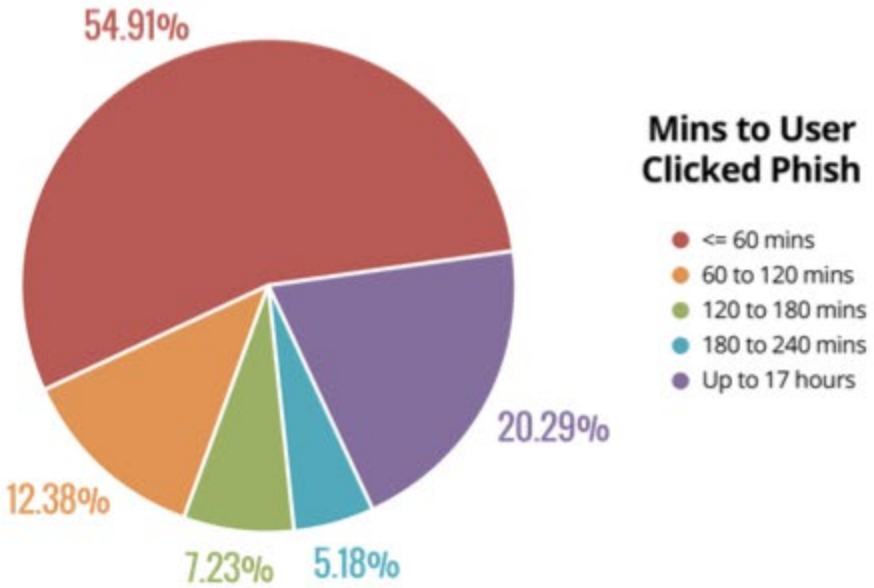
Source: Microsoft Security Intelligence Report, Volume 24 January - December 2018

Recent studies show that over

54.9%

of users click on a phishing link in under 60 minutes

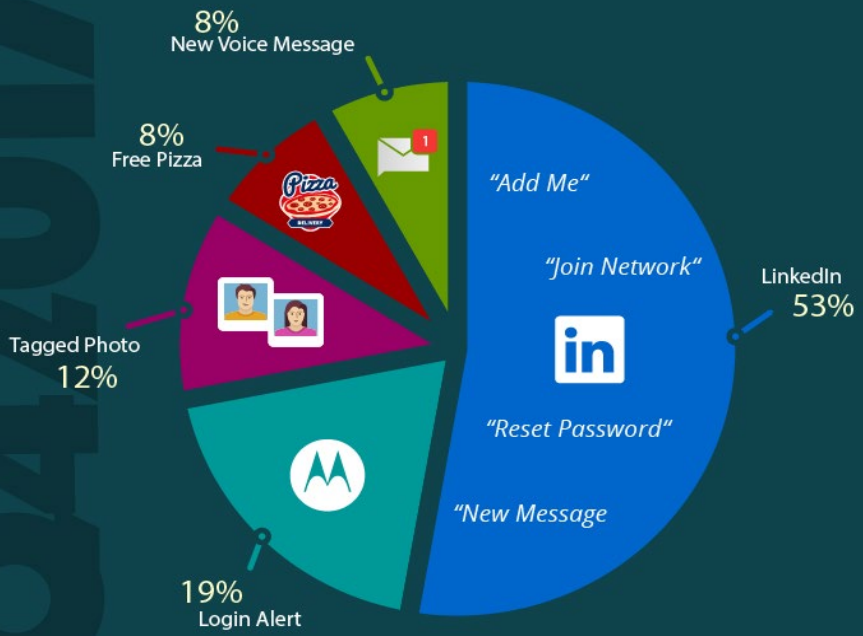
Why Do People Click On Phishing Links So Quickly?



KnowBe4
Human error. Conquered

TOP-CLICKED PHISHING TESTS

TOP SOCIAL MEDIA EMAIL SUBJECTS



TOP 10 GENERAL EMAIL SUBJECTS

A Delivery Attempt Was Made	18%
UPS Label Delivery 1ZBE312TNY00015011	16%
Change of Password Required Immediately	15%
Unusual sign-in activity	9%
Happy Holidays! Have a drink on us.	8%
Join my network on LinkedIn	7%
Staff Review 2017	7%
All Employees: Update your Healthcare Info	7%
Psst. PSL is B-A-C-K!	7%
Invitation: Performance Review	6%

KEY TAKEAWAY

Email is an effective way to phish users when disguised as legitimate email. These methods allow attackers to craft and distribute enticing material for both random (general phish) and targeted (spear-phish) means, leveraging multiple psychological triggers and engaging in what amounts to a continuous maturity cycle.

COMMON "IN THE WILD" ATTACKS

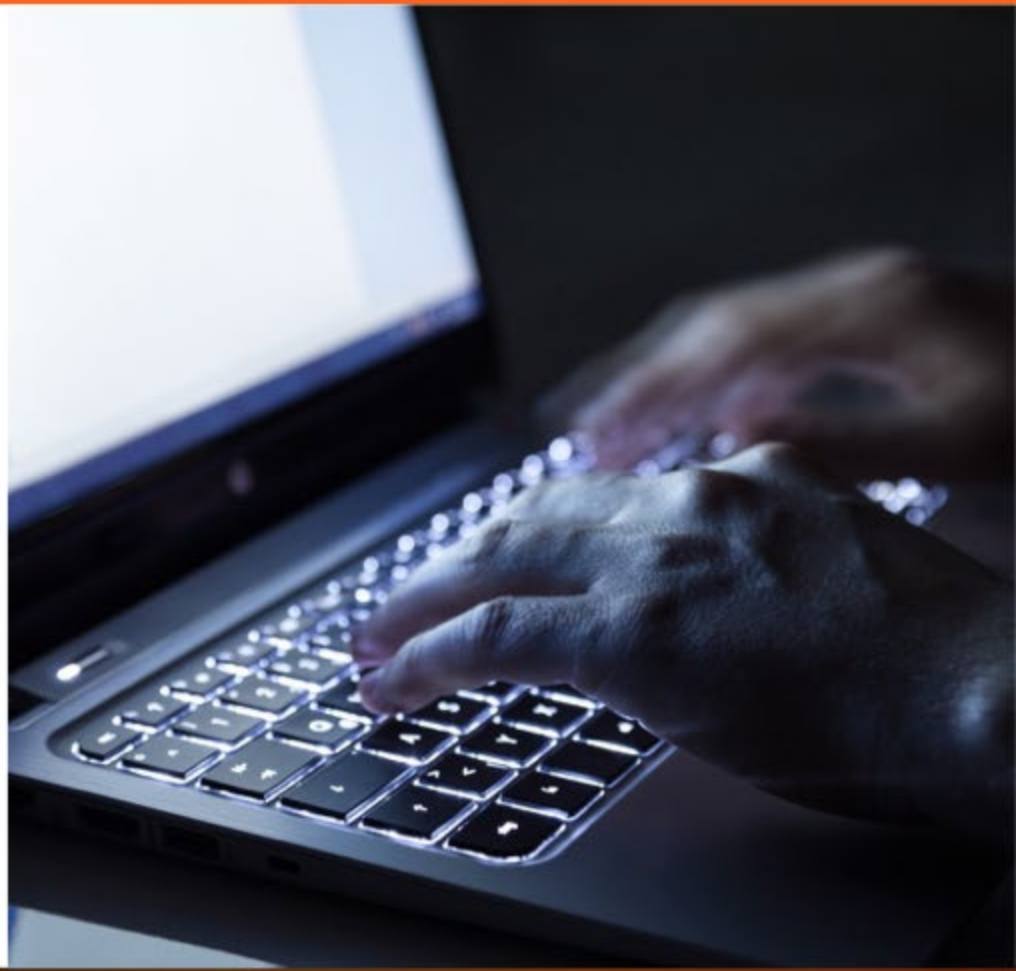
- Microsoft Drive: Invoice&payment21.pdf
- ID Suspension
- Your domains have been blocked
- Microsoft Office 365 Upgrade Test
- Facebook: Secure your Account
- PayPal: Your account was recently logged into from a new browser or device
- HR: End of year payroll Adjustment
- Alibaba.com: Lisa Witt has sent you an inquiry
- Microsoft Outlook: Inbound Activity Error: Failure receiving mail [Case ID: 39900801]
- Your iCloud account was used to login from a new device and location

The Cost of Clicking

- The loss of data, including intellectual property can cripple an organization
- Reputation damage can be significant
- Price per record - $158 ($355 for healthcare) per stolen record
  (IBM 2016 Cost of Data Breach Study)
- Typical price per breach - $861,000 for large businesses and $86,500 for SMB (Kaspersky - September 2016)
- Man-hours spent - 22-38 hours of labor to resolve
  (SentinelOne)

Your Employees Are Your Last Line Of Defense

- **91%** of successful data breaches started with a spear phishing attack
- **CEO Fraud** (aka Business Email Compromise) to exceed $12.5 billion in damages in 2019
- **W-2 Scams** social engineer Accounting/HR to send tax forms to the bad guys
- **Ransomware** damage costs predicted to reach $20 billion by 2021



HOW CEO FRAUD IMPACTS YOU

THE START

Attackers see if they can spoof your domain and impersonate the CEO (or other important people)

Bad guys often troll companies for months to gather the data necessary in pulling off a successful attack

THE PHISH

Spoofed emails are sent to high-risk employees in the organization

To: Finance Department

Urgent wire transfer request! Please send $100,000 to new acct #987654-3210

To: CFO

Please pay this time-sensitive invoice. I'm on vacation and will be unavailable, no need to respond. - Your CEO

To: Human Resources

I need a PDF copy of ALL employee W-2s for the IRS ASAP!

THE RESPONSE

Target receives email and acts without reflection or questioning the source

I better get this payment to the new account!

It's from the CEO, I'll take care of this for him!

Sounds important. I'll send these right away!

THE DAMAGE

Social engineering was successful, giving hackers access to what they were after

Causing fraudulent wire transfers and massive data breaches

THE RESULT

The fallout after a successful attack can be highly damaging for both the company and its employees

Resulting damage:

- ✓ Money is gone forever in most cases and only recovered 4% of the time
- ✓ CEO is fired
- ✓ CFO is fired
- ✓ Lawsuits are filed
- ✓ Intangibles - tarnished reputation, loss of trust, etc.

So... Think Before You Click!

SECURITY AWARENESS TRAINING | www.KNOWBE4.COM

Comprehensive Programs Work

- Most security awareness programs are still **too superficial** and done for compliance reasons.
- What is missing is the **correct estimation of the adversary** being faced and the degree of commitment an organization has to have to stave off attacks.

How Do You Manage the Ongoing Problem of Social Engineering?

Baseline Testing
We provide baseline testing to assess the Phish-prone™ percentage of your users through a free simulated phishing attack.

Train Your Users
On-demand, interactive, engaging training with common traps, live hacking demos and new scenario-based Danger Zone exercises and educate with ongoing security hints and tips emails.

Phish Your Users
Fully automated simulated phishing attacks, hundreds of templates with unlimited usage, and community phishing templates.

See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!

Questions?

Contact: Tiffany Yeager
727-877-8226
tiffanyy@Knowbe4.com

KnowBe4
Human error. Conquered.