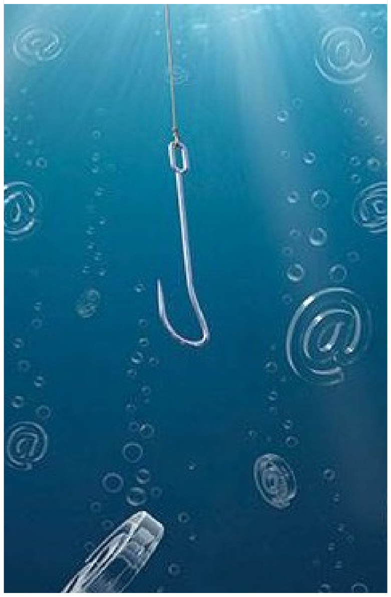
Merchant Link, LLC.
8401 Colesville Rd., Suite 900
Silver Spring, MD 20910

Phishing Training

Detecting and Avoiding Phishing Attacks



Merchant Link

Merchant Link Learning and Development

Merchant Link, LLC
Learning and Development
8401 Colesville Road, Suite 900
Silver Spring, MD 20910

This manual is documentation of the Learning and Development department of Merchant Link, LLC. This document is based on proven best practices, national and international statistical reports and data regarding security threats, breaches, and defensive best practices. This document is supportive material for our Anti-Phishing training initiatives. This guide is in no way intended to be an all-inclusive document.

DO NOT REMOVE THIS PAGE

Table of Contents

Introduction

Welcome to our Anti-Phishing instructor-led training course.

Course Agenda

- Phishing overview and types of attacks
- Identification of phishing emails
- Consequences to falling prey to phishing
- Human Behavior and Cyber Security

Objectives

After completing this course, you will:

- Understand the types of phishing attacks and how to identify them.
- Understand how personal work habits contribute to secure behaviors.
- Understand the consequences of falling victim to phishing attacks.

Phishing

Overview

Phishing is a form of fraud where cybercriminals attempt to collect information from a user by posing as a legitimate source (e.g., financial institution) to steal personal information, money, financial data, trade secrets, or gain access to computer systems, among other activities.

In phishing attacks, cybercriminals utilize manipulation and deception to trick users into providing the requested information (i.e., social engineering). Such tactics make it difficult for users to accurately identify fraudulent emails. In fact, only 3% of the more than 19,000 people from around the world that took Intel Security's 2015 Phishing Quiz identified every phishing email correctly; and 80% of quiz takers incorrectly identified at least one phishing email.

Given that it only takes one email to fall victim to a cybercriminal's attack, it is important for you to understand:

- the potential impacts on victims;
- the tactics used in phishing scams; and
- Behavioral modifications that users can implement to protect themselves and their families, friends, schools and employers.

This page left blank intentionally

How Phishing Impacts YOU

Cybercriminals may use phishing techniques to steal credentials (e.g., usernames, passwords) and other personal information to gain access to personal or work accounts to steal money, financial or health data, trade secrets, or other sensitive information, or to carry out other crimes, such as identity theft, corporate espionage, or extortion, among other acts.

The information obtained through phishing can also lead to further victimization. For example, if a user's personal information (e.g., name, address, telephone number, email account) is posted online; other criminals may use this information to commit other crimes against the victim (e.g., stalking, harassment, burglary).

Victims may even be at risk of becoming suspects in crimes committed by a criminal using their identity or credentials. For example, the cybercriminal may use the victim's credentials to steal money from their employer through an illegal wire transfer.

Both the personal and professional lives of the victims of cybercrimes can be impacted in a wide range of ways, such as:

- lost time
- trauma
- financial loss
- social consequences
- business consequences
- lost productivity

Lost Time

Recovering from a phishing attack can be confusing, time consuming, and generally inconvenient for victims. Depending on the type of damage caused by a phishing attack, victims can spend anywhere from a few hours to many months or years resolving the associated problems.

Trauma

Phishing attacks can cause significant emotional distress (e.g., denial, loss of trust, frustration, fear, anger, powerlessness, helplessness, embarrassment, depression, sleep disturbances). Some theorize that cybercrime victimization, such as identity theft, can be more harmful to victims than crimes like property theft because one can replace property, but it is not possible to acquire a new identity.

Further, phishing victims can experience stigmatization by others who blame the victim for falling for the attack.

Financial Loss

Victims can incur both direct (i.e., value of goods, services, or cash obtained) and indirect (e.g., legal fees, bounced checks, postage) financial loss resulting from phishing attacks. For example, in 2014, victims of identity theft reported an average combined direct and indirect loss of **$1,343**.

In addition, the employers of phishing victims can experience financial losses related to decreased productivity (see below), business disruption, isolating malware and credential compromises, and the cost of data breaches. Researchers estimate that the total annual cost of phishing for the average company is $3.77 million.

Social Consequences

Victimization can cause strain on personal and family relationships and reputational damage. For example, if cybercriminals gain access to a victim’s email, they can uncover information about personal relationships or embarrassing photos or videos that may be leaked to the public. Family or friends could also become the targets of cybercriminals.

Business Consequences

Both intellectual property and customer data can be at risk when a phishing attack occurs. In addition to financial loss, a phishing attack can damage the reputation and credibility of a business. Consumers may lose trust in the business, which can lead the company to lose its customer base.

Moreover, cyber-espionage typically begins with phishing when employees interact with malicious attachments or follow links to malicious websites. This initial attack allows cybercriminals to gain backdoor access and install malware on computers/devices to further penetrate a system network.

It can take months to years to detect a network compromise and it only takes minutes to steal information off a network, cybercriminals can have long periods of undetected access to trade secrets that can hinder business growth.

Lost Productivity

The time it takes to recover from a phishing attack and the trauma inflicted can result in decreased employee productivity. It is estimated that non-IT employees spend an average of 4.16 hours per year dealing with phishing attacks.

The related cost of productivity losses is estimated to be $1.8 million—accounting for 48% of the total organizational costs.

Further, productivity can also be lost in preventing phishing attacks, as employees spend time determining if an email is fraudulent.

Types of Phishing

Click only

This technique employs a simple hyperlink directing the user's Internet browser to a malicious website that may exploit a bug in the browser or in Java to run code on the user's system and compromise the entire OS.

Data entry

This phishing attack takes the malicious hyperlink a step further by directing the user to a site that is collecting information. The email will contain language and some information to set a frame of mind in the user so that they willingly provide personal information or login credentials to the malicious site. For example, a bogus email from a banking institution asking the target to update their account information after logging into the system.

Attachment

This attack method employs malicious attachments such as Word documents, office documents, PDFs or other files to compromise a target's system. Often these will be files made to look like invoices or other business related documents that the email is asking you to review in resolving some kind of issue. The simple act of opening these documents is all it takes to compromise a system and an entire network.

Double barrel

This begins with sending one benign email (the lure) that is innocuous and does not require any response from the victim. It could be a simple introduction such as:

> *`Hi, we met at CES last week and had a great conversation! I have a white paper I'd like to share with you based on what we talked about and will send it over shortly.'*

A little later on, the aforementioned white paper appears and the victim is now prepared to receive it.

Note that the delivery order can also be reversed. The goal is to send the lure ***before*** the malicious email in order **to give the victim a sense of confidence** in the whole experience. Social engineering is at the heart of *every* phishing attack.

Why is Phishing So Successful?

Phishing attacks often rely on a combination of tactics that are known to influence human decision-making, such as:

Authority

Research has found that people tend to comply with requests from authority figures. Phishing frauds claim to be from a trusted source by using a corporate logo or name as the sender to attempt to create legitimacy and credibility.

Time Pressure

Phishing frauds may request a rapid response to pressure users to act quickly, and decrease the time users have to uncover the fraud.

Tone

Phishing frauds often use a formal tone with a combination of persuasive and polite statements to influence user decision making. Examples include polite salutations and closures (e.g., Dear, Thank you, Kind regards); trigger words (e.g., alert, warning, attention); and persuasion (e.g., upon verification, restrictions will be removed).

Salient Pieces of Information

Phishing frauds may include a personalized message or salient pieces of information (e.g., primary account contact) to persuade a user that the email is legitimate. In targeted phishing attacks (i.e., spear-phishing), cybercriminals build a target profile based on public information (e.g., employer websites, social media) to craft more authentic appearing messages. By acquiring key insider knowledge (e.g., job functions, work relationships), cybercriminals can increase the likelihood of a successful attack.

Fear

Phishing frauds may prey on users' fear of something to manipulate them into acting. Cybercriminals may invoke fear by making threats (e.g., account restrictions) or leveraging current events (e.g., natural disasters, health epidemics, economic concerns, political elections, holidays, etc.).

Phishing vs. Spear Phishing

Phishing attacks and spear phishing have much in common, including the shared goal of manipulating victims into exposing sensitive information. Spear phishing attacks differ from typical phishing attacks in that they are more targeted and personalized in order to increase chances of fooling recipients.

Attackers will gather publicly available information on targets prior to launching a spear phishing attack and will use those personal details to impersonate targets' friends, relatives, coworkers or other trusted contacts. Information that attackers can leverage for spear phishing includes victims' employment information, organizations that they belong to, hobbies, and other personal details.

Much of this information can be gleaned from targets' profiles and/or activity on social media sites. In many cases, spear phishing attacks are used as a first step in an Advanced Persistent Threat attack targeting a specific organization.

Human Behavior and Cybersecurity

Overview

Preventing Phishing Attacks Requires Behavioral Change

In general, phishing attacks rely on a combination of behavioral factors to influence users. How individuals perceive risk can explain why users exhibit poor security habits. For example:

- Users may be overconfident, believing that they will not be the target of a cyber-attack (i.e., optimism or normalcy bias), decreasing the likelihood that a user will seek additional information to determine the legitimacy of the request (e.g., checking the email address, calling the sender)
- Users may believe that cybersecurity is not an issue relevant to them because they have not been a victim or known a victim, leading them to delegate cybersecurity measures to others such as I.T. and Enterprise Security.
- Cognitive biases can make users more vulnerable to phishing attacks. Therefore, users must incorporate behavior changes into their regular online activities to prevent successful phishing attacks.
- Work habits may contribute to vulnerabilities such as multi-tasking or “reflexive” application usage.

Why Behavior Matters in Cybersecurity

Cybercriminals use phishing and social engineering to defeat data and system security by exploiting weaknesses in decision-making and human behavior.

> *Approximately 95% of cyber-attacks and events involve preventable human error and behavioral weaknesses.*

This number suggests that Internet users are vulnerable, **independent of platforms and software**. As behavioral scientists have argued, psychology plays an important role in providing answers to why individuals engage in risky cybersecurity practices. Therefore, there are cybersecurity areas and problems where behavioral science can be applied to create a positive impact on users’ cybersecurity habits.

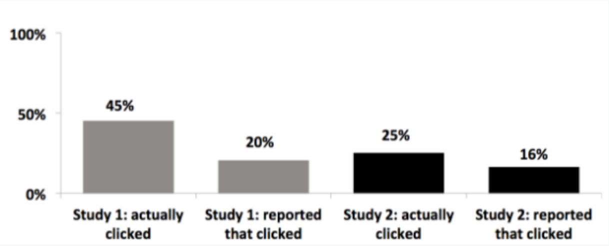
Secure behavior relies on decision-making. Internet users must be aware of the ways their behaviors and decision making expose them, their family, and the company to cyber-threats.

Arun Vishwanath, associate professor of communication at the University at Buffalo, has done social-psychological research on phishing and found **"ineffective cognitive processing"** to be the key reason victims fall for fake emails.

"**Even after training to detect deceptive emails, people tend to quickly sink into bad habits."** he said.

Risk beliefs, including misperceptions about device security, are another factor. "We ask people, what do you think is safer, a PDF or a Word document?" Vishwanath said. "What do you think is safer, an iPhone or Android device?

People have these beliefs about what is safe and what is not, and most of them have nothing to do with malware attacks." iPhone users, for instance, are more likely to click on malicious links than Android users, falsely believing they are safe.



78% of people claim to be aware of the risks of unknown links in emails. And yet they click anyway.

Friedrich-Alexander University (FAU)

Continual awareness training can *help* to inform on the latest trends and techniques but there **must be a change to the casual use of technology and the assumption that I.T. "Has our Back"** and that simple patching can prevent all exploits and vulnerabilities.

*We must shift from Security **Awareness** to Security **Action***

Evaluating Risks

When looking at your day-to-day work, what are the most hazardous activities and tools you encounter? It is true that there are countless ways that you can fall prey to malicious activities, but what are the most likely you will encounter?

If you were to choose two of the most “dangerous” tools or activities, what would they be, and why?

1. ____

   ____

2. ____

   ____

What Do We Fear?

They say fear is a motivator. So, how does the possibilities of being breached through a phishing attack stack up with other concerns that society, or we, have? When faced with the statistics, do we adequately understand how vulnerable we are?

Take the following situations and think about you own concerns. Do you feel more or less susceptible to these eventualities? Rate your level of concern (With 5 being the greatest level of concern) against each entry and enter your guess on what the odds are of the event happening to you.

What are the Odds?						
Event	**Level of Concern**					**Estimated Odds**
Being the victim of a ***single*** phishing attack	1	2	3	4	5	
Being the victim of phishing	1	2	3	4	5	
Being the victim of a terrorist attack	1	2	3	4	5	
Dying due to accidental poisoning	1	2	3	4	5	
Dying in a car accident (annually)	1	2	3	4	5	
Child being born with extra fingers or toes	1	2	3	4	5	
Being murdered	1	2	3	4	5	
Dying as a pedestrian	1	2	3	4	5	
Having identity stolen	1	2	3	4	5	
Dying from a lightning strike	1	2	3	4	5	

Phishing Prevention Tips

Several techniques that are simple to understand and exercise can help protect you from becoming a victim. The following tips, when incorporated into your daily life, will provide a significant improvement in securing against phishing.

Check the Sender

- Are the name and the email address the same? (e.g., the "from" address text says the institution's name but the email address does not.)
- Does the email address have the same domain name as the company's website? Look out for variations in spelling and domain (.com, .net).
- Unsure? Contact the sender or company directly using information on your account statement or found online. Do not use the email address, phone, or website included in the message.

Identify the Recipient of the Email

- Does the salutation include your name?
- If it includes salient pieces of information, are those accurate? (e.g., are you the primary contact on the account?)
- Does your name appear in the "To:" address line or are there variations in the CC: line?

Carefully Read the Message

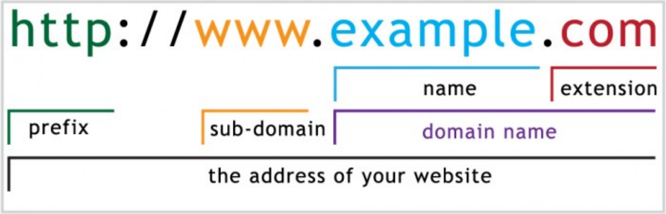
- Does the message contain errors such as typos and poor grammar?
- Does the message contain threats or invoke fear?
- Does the message request an urgent action?
- Does the message ask you to log into a site or application?
- Does the message imply you must provide information the site should already have expecting you to confirm or change it?

Know Where the Links Will Take You

- Check the URL before clicking any link
  (Hover over the hyperlink with the mouse pointer. In mobile applications, you may or may not have this luxury.)
- Do the hyperlinked text and the URL match?
- Is the domain in the URL the same as the company's website?
- Look out for variations in spelling and domain (.com, .net).
- Look for similar looking text attempting to dupe you into trusting them (i.e. www.rnicrosoft.com, www.h0tmail.com, www.goog1e.com)
- Type the website address into a browser manually instead of clicking the link.

What's in a URL?

Understanding the basics on how a web domain address is constructed can go a long way in determining whether a link is legitimate, or a potential hazard.



Prefix

The URL prefix identifies the **protocol** that is being used. This includes standard web pages and secure sites (http/https), File Transfer Protocol or FTP, streaming media services (smtp) or other technologies.

Sub-domains

Sub-domains point to computers or instances of web servers within a company's domain. These could be servers handling normal web pages (www), web-based email servers, vpn services or more. Sub-domains can be named anything the domain owner desires.

Name

The name of a domain is the most recognizable part of the URL, generally being the name of the corporation or entity. (Merchant Link = merchantlink). This can be anything the domain registrant desires as long as it has not been reserved already.

Extension

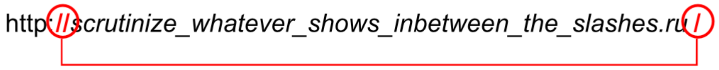
In all but the rarest cases, this is typically a ".com", or commercial extension. Since that is one of the oldest and most recognized extensions, it is rare to see any company of repute or significant size to be using a different extension for their primary web presence. Extensions can also be identifiers of the nation or region such as .uk or .ru for England and Russia.

Top Level Domain (TLD)

These terms refer to the Name and Extension as a combined entity (merchantlink.com) Depending on what is being discussed, the TLD or Top Level Domain may be referring to only the extension in an URL. The "top – down" concept of an address starts at the extension and works its way to the left, becoming more specific as it goes. TLDs are registered typically to a company in a specific geographic region.

Prefix	Subdomain	Name	Extension
http ftp https	www email vpn ftp	merchantlink microsoft yahoo google ibm	com us ru biz org gov

Look between the slashes


http://scrutinize_whatever_shows_inbetween_the_slashes.ru/

When trying to detect a legitimate URL you will look for the first instance of a forward slash AFTER the **http(s)://** of the URL. The entry between these forward slashes will be the Fully Qualified Domain Name (FQDN) for the site you are interacting with. From the slash, work your way from ***right to left*** to identify the parts of the URL and its legitimacy

Examples of spoofed or bad web addresses

- http://paypal.custsupport.co/login.com
- http://bofa.com.sa/bankofamerica.com/5d55d6cdaf3de13394d4
- http://my.bluehost.com.ef35613fc5fa.confirmation.bitte.19.in.ua/dir/cgi.html?action=54d56f56

Know Your Merchant Link Domains

There are a number of domains that we interact with that you should know and be on the lookout for. The following are some of those domains including partners for HR related resources:

Subdomain	Domain	Application or site
*** www	**merchantlink.com**	VPN gateway Corporate web page
***	**merchantlink.us**	Microsoft Dynamics CRM
****	************.com**	Testing server
merlin **** teamsite ****** jira ithelpdesk	********.********	MerLin SharePoint Intranet Support tools for MerLin on SharePoint Various SharePoint sites outside of MerLin ******************** Jira project management tool SysAid
workforcenow	**adp.com**	Employee payroll site
merchantlink	**giveawow.com**	Employee recognition partner site
system	**netsuite.com**	NetSuite tool
merchantlink	**mybenefitsview.com**	My Benergy employee benefits web portal
www	**rps.troweprice.com**	T. Rowe Price 401k Portal
Member	**carefirst.com**	CareFirst portal
www	**caremark.com**	CareMark portal
www	**metlife.com**	Metlife dental benefits portal

Think Before You Click Links or Open Attachments

- NEVER open attachments or click links that you are not expecting.
- While the I.T. group and Enterprise security ensure your anti-virus software/security settings are up-to-date and enabled, ***never assume that you are protected***. Treat ***every*** link and attachment as a potential attack. Break the cycle of vulnerable work habits

Using familiar applications such as Outlook and Word can contribute to our vulnerability. When performing common tasks, the human mind tends to "skip ahead" with a tendency to anticipate and "pre-respond" to application dialogs and interfaces. When using these applications it can become almost automatic to open and click through since the mind is scanning for the new and important information. This creates a sort of "Reflex" in the mind.

For instance, recently an FBI official admitted that the head of security at his office failed a phishing test she had administered, **because she was multitasking**. **People also forget their training and the lessons from phishing tests**.

Changing our perception of Outlook or other email tools can be the first step to fortifying ourselves against these exploits. These tools should be the last applications where we shift into "auto-pilot" since they are the primary door phishers use to gain access. Try remembering the following whenever you are using Outlook:

> *Pause, Think, Act.*

Distracted Driving is Bad…

So is **Distracted Computin**g. Changing how you perceive and use email is the start to securing your behavior, but what are the effects of other office distractions that may affect your security-mindedness?

Consider the following behavioral changes:

- Email is very distracting if you are reactive to it. Set a schedule and stick to it: e.g. check emails not more than once an hour; determine the priority of replies/actions to be taken based on new email and only perform the critical ones right away, otherwise "park" them and get back to the task you were doing.

- Make sure you have filters set up in your email to ensure that anything not so important does not get in the way, so these messages skip the Inbox. Then only check the rest of the email (which has been filtered) at set times (like start and/or end of the day).

- Separate work and personal communications to eliminate friendly distraction.

IF YOU THINK YOU HAVE BEEN A VICTIM OF CYBERCRIME

- Change Your passwords immediately
- Contact the real institution(s) where YOU have the account
- Report the incident to the CSIRT

Self-Assessment Activity

1. Using the following worksheet enter an identified vulnerability or security practice with regards to Phishing that you need to work on for each commitment area.
2. Identify the “Patch” to your practices that will be applied to the vulnerabilities or practices you identified.
3. Turn this worksheet into your manager within one week of completing this Instructor-led training session. Completion of this activity is required.

Activity

Commitment Area	Security Vulnerability or Behavior	Actions Needed to Correct
Changes to Work Habits: What work habits can you improve to become more secure?		
Improved Threat Identification: What technical limitations do you need to improve upon?		
Technical Gaps: What technical subjects do you feel you do not fully understand?		

Name: ______________________________ Date: __________

Manager: ______________________________ Date: __________

Course Instructor: ______________________________ Date: __________