KnowBe4
Human error. Conquered.

E-BOOK

Comprehensive Anti-Phishing Guide

About This Guide

This ebook is a comprehensive guide to help fight social engineering and phishing. It covers the needed policies, technical defenses, and best practice security awareness training tips, which if implemented, will significantly reduce cybersecurity risk due to social engineering. Using security awareness training, especially the way KnowBe4 enables it, is one of the most significant and best ways to fight social engineering and phishing. It is, however, just one major part of an overall, more comprehensive, strategy. If you've been looking for an all-in-one-guide to fight phishing, this is it. No guide can be guaranteed to cover everything, but this document attempts to cover as much as is reasonably possible.

Note: Much of the content in this ebook is covered in a one-hour KnowBe4 webinar if you prefer to learn visually/aurally.

The Need to Fight Social Engineering and Phishing

Social engineering and phishing are responsible for 70-90% of all malicious digital breaches. There are many ways a system, network, or individual can be attacked (e.g., eavesdropping, man-in-the-middle attack, software bug, denial-of-service, physical attack, etc.), but by far the most common method is social engineering and phishing. Exploitation of unpatched software bugs follows in a distant second place, involved in 20% to 40% of all digital breaches.

Social engineering and exploiting unpatched software have been the number one and number two most successful hacking methods for decades.

Together, social engineering and unpatched software account for 90% to 99% of cybersecurity risk in most environments. Every other type of cyberattack only accounts for 1% to 10% of cybersecurity risk. The percentage of the overall cybersecurity risk that social engineering is involved in changes over time, but it is almost always the top threat listed by any data source.

KnowBe4 did a meta-survey of 100 other cybersecurity studies which collected, ranked, and published root exploit causes. The end result was that regardless of the percentages published in any individual report, social engineering was the top root exploit cause listed of most reports and was by far the number one threat when aggregated across all reports. This ebook will help you to most efficiently fight social engineering and phishing, which is the single best thing most organizations can do to best reduce cybersecurity risk the fastest.

No matter whose data you rely on, it is clear that there is nothing any organization or individual can do to decrease cybersecurity risk faster and better than to fight social engineering and phishing.

Table of Contents

EFFECTIVELY FIGHTING CYBERSECURITY ATTACKS

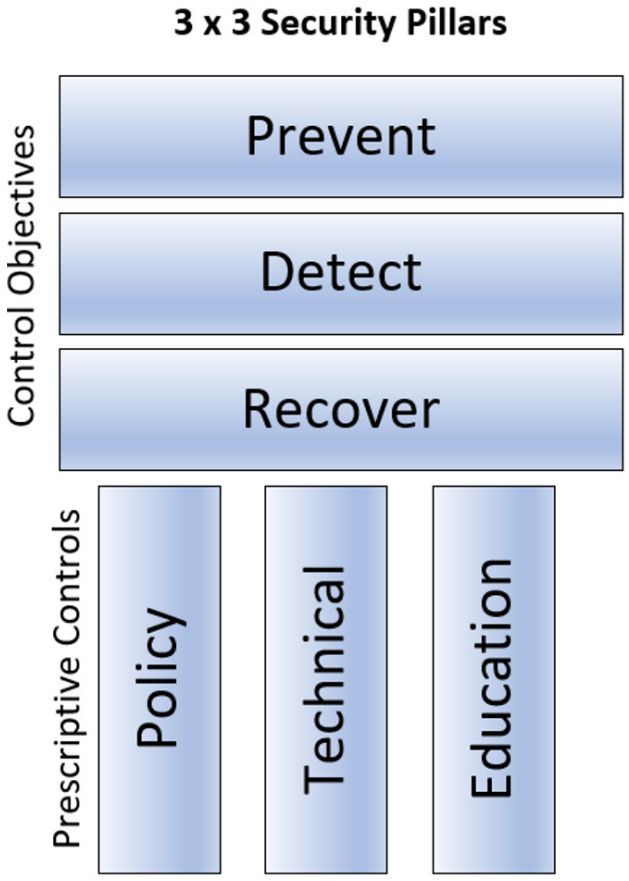
Effectively fighting cybersecurity attacks takes the best, defense-in-depth, combination of policies, technical defenses, and training possible. Security policies are the effectively and consistently communicated instructions, recommendations, and procedures that a stakeholder should follow to most effectively eliminate risk and the chance of a threat being successful. Policies can be verbal, written, exampled by behavior, or posted online, and require attestation of understanding of the stakeholder. They can be voluntary recommendations or required (sometimes by law).

Technical defenses are all the physical and logical mitigations and controls implemented to prevent something harmful from happening. In the digital world, this often refers to logical implementations due to hardware devices (like firewalls, etc.), operating systems, and applications. Technical defenses are great at blocking large percentages of previously recognized, broad types of attacks.

Training is all the actions taken to teach another person a particular action or behavior. Security awareness training, in particular, is education used to make a person aware of a particular type of threat to make them less likely to be involved in the success of a malicious exploit. Some amount of social engineering and phishing will always get past your policies and technical defenses, so training is needed to help users recognize threats and to take the appropriate actions.

These mitigations should be used first and foremost to prevent a threat from being successful. Mitigations which stop a threat from being successful are known as preventative controls. Even with the best defenses, it is difficult to prevent all threats and attacks from being successful. It must be assumed that an attack may be successful from time to time, getting past your best preventative controls (an idea known in the computer world as "assume breach"). If an attack is successful, you want to be able to, as quickly as possible, detect that an attack has successfully gotten past your preventative controls to get early warning of a successful breach (using detective controls). The earlier the warning, the higher the opportunity to remove the threat and reduce potential damages. Once an exploit is detected, all reasonable effort should be made to stop continuing damage or expansion, to remove the threat, and analyze and/or update the list of preventative controls which allowed a threat to be successful.

So, as summarized in the 3 x 3 Security Pillars in the figure below, organizations should implement the best cost/benefit combination of policies, technical defenses, and training, possible to appropriately mitigate the majority of risk. The biggest, most likely, and potentially most costly threats should be mitigated first and best. Given the fact that social engineering and phishing are the biggest threats in most organizations, this means that most organizations should strive to mitigate social engineering and phishing threats first.



Effectively fighting cybersecurity attacks takes the best, defense-in-depth, cost/benefit-justified, combination of policies, technical defenses, and training possible.

The rest of this ebook will give a comprehensive list of mitigations. Not all mitigations will or can be implemented by all organizations. This ebook is intended as an inclusive summary of the most common policy, technical defenses, and training best practices that any organization can avail themselves of. Readers should use this ebook as a guide to learn about what other organizations do to fight social engineering and phishing and to locate and resolve potential weaknesses.

POLICIES TO FIGHT SOCIAL ENGINEERING AND PHISHING

This section summarizes the policies that any organization should have to effectively fight social engineering and phishing. They include Acceptable Use Policy and specific anti-phishing policies.

Important: Any adds/deletes/changes to any policies or documents need to be reviewed by your management and legal teams before implementing.

Acceptable Use Policy

Every employee should read, acknowledge, and sign an Acceptable Use Policy (AUP) when hired, and annually thereafter. An AUP is a general IT policy document to educate users and other third parties (e.g., contractors, vendors, etc.) who may use the organization's IT resources or handle protected data, about what is allowed and is not allowed regarding the organization's IT devices, networks, services, and data, including personal responsibilities.

An AUP covers far more than anti-social engineering policies, attempting to cover overall general IT "do's and do not's" in a holistic manner. An AUP often includes a scope, a statement of general overarching governance philosophy, a code of conduct, examples of what is allowed, what explicitly isn't allowed, and consequences of failing to meet acceptable use policies. As examples, common general policies included in most AUPs include "Don't give your password to others" and "Lock your desktop when you are away from your desk".

AUPs vary greatly depending on the organization being covered, the business conducted, and the participant's relationship and appropriate expectations. For example, AUPs for educational facilities tend to focus on students and teachers, whereas most organizational AUPs focus on employees and vendors. Regardless of the type of organization involved, there are many AUP examples on the Internet, including:

- https://www.getsafeonline.org/themes/site_themes/getsafeonline/download_centre/Sample_Acceptable_Usage_Policy.pdf
- https://www.isc.upenn.edu/IT/policies
- https://www.earthlink.net/acceptable-use-policy/

Every organization should have an AUP and have it reviewed and signed by every stakeholder, when hired, and annually thereafter. Ensure that your organization has an AUP signed by every stakeholder. If not, create one and have it reviewed and signed by all stakeholders, both present and future.

Specific Anti-Phishing Policies

An AUP may or may not cover policies designed to mitigate social engineering or phishing. An AUP should cover at least the minimum basics, such as "Don't open unexpected file attachments, especially from unknown email addresses" or "Never give out your login in response to an unexpected email", etc. In some organizations, an AUP is the first, and sometimes the only, opportunity to educate a stakeholder in how to successfully fight phishing and social engineering.

Anti-phishing content is often covered in other security policies. However, it is implemented, specific anti-phishing policies should be covered and frequently communicated to stakeholders. Anti-phishing policies should be directed at general awareness of the threats, specific education on the related topics, common examples, and education on how a stakeholder should recognize and treat suspected social engineering and phishing. Succinctly, anti-phishing policy should focus on how a stakeholder should recognize and treat phishing threats.

A specific anti-phishing policy should include at least the following:

- A specific recognition of the great threat that phishing and social engineering pose to the environment, including risks from a successful breach
- Definitions
- Examples of common phishing and social engineering attacks
- Specific anti-phishing actions and behaviors to help mitigate risk

Note: Policies are part of a stakeholder's education and dovetail with the general information and best practices summarized in the section entitled Training Best Practices to Fight Social Engineering and Phishing published further below.

Examples, Policies and Phrasing

Here are some example policies and phrases which can be included in an anti-phishing policy section.

Introduction

Every security policy should indicate the significance of the threat of social engineering and phishing so that stakeholders understand the importance of paying particular attention to related security policies and actions. An example stated policy objective can begin like this:

> *"This organization recognizes that one of the most popular and damaging hacking methods any organization can be maliciously compromised by is social engineering and phishing..."*
>
> *"Risks of a successful exploitation include: unauthorized system access, denial of service, data exfiltration, reputation issues, attacks against our employees and customers, stolen IP, fines, financial harm, etc."*

Definitions

Every anti-phishing security policy should clearly define social engineering, phishing, and other related terms so readers have a clear understanding of the threats. Definitions which should be included: Social Engineering, Phishing, Spear Phishing, Ransomware, CEO Wire Fraud, Smishing, Vishing, Patching, etc. Here are two example definitions you can use:

> **Social engineering** is the act of deceptively manipulating people into performing actions or divulging login information or confidential information contrary to their or their organization's best interests. Social engineering can be performed in person, using a paper-based delivery method (like the postal service), over a phone, or digitally/online.
>
> **Phishing** is a type of social engineering which typically refers to digital and online methods, including: email, websites, instant messaging, and Short Messaging Service (SMS) text messages, but it can also include voice calls (i.e., vishing). The most common methods involve sending fraudulent emails to potential victims or tricking website visitors into divulging login information or into running Trojan Horse malware programs. The threat of social engineering and phishing is a significant problem in every country and organization.

A comprehensive glossary pertaining to phishing and other cyber definitions, including those above can be found here: https://www.knowbe4.com/knowbe4-glossary/

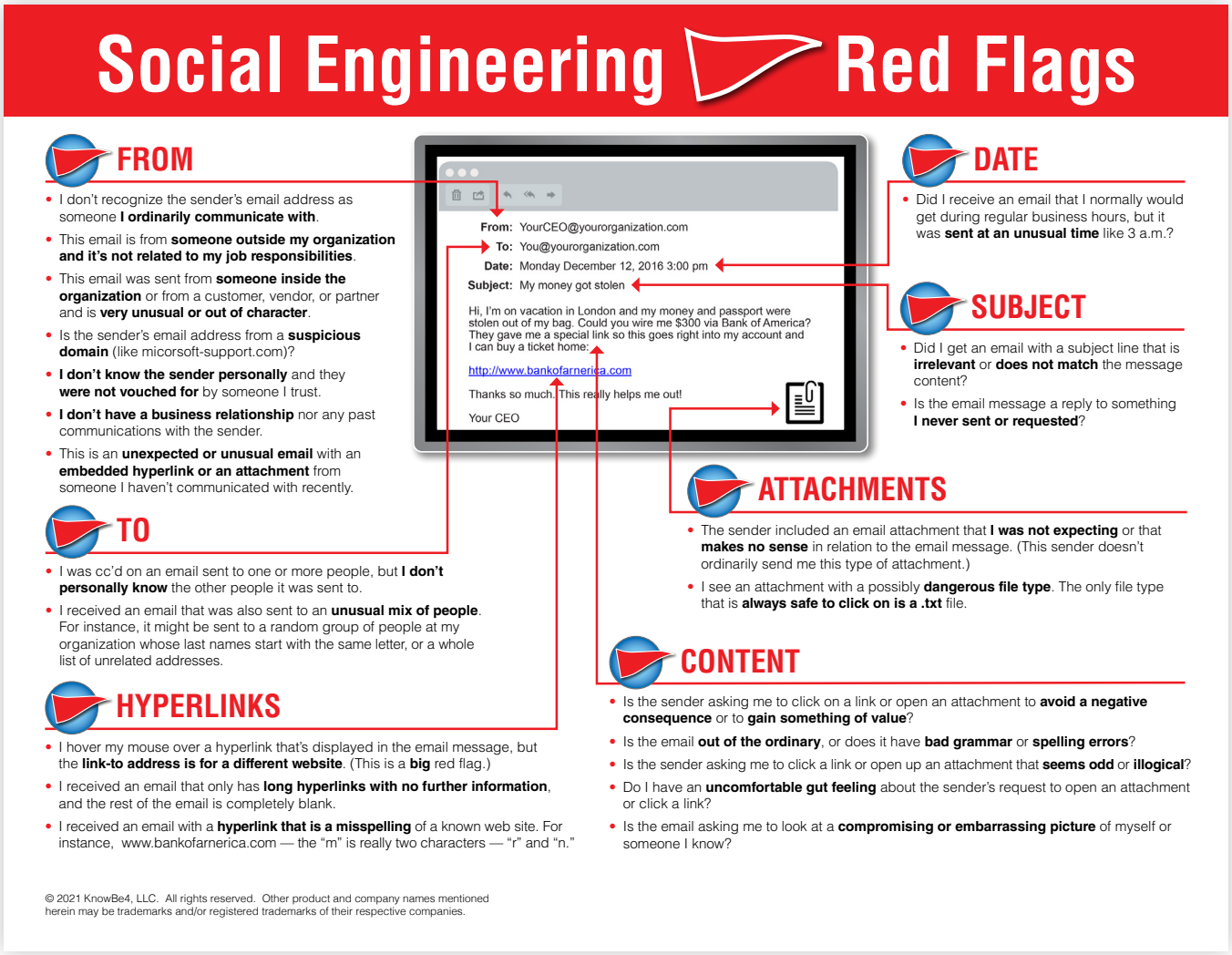
Recognizing Common Social Engineering Red Flags

It is essential that all employees be taught how to recognize the most common signs of phishing and social engineering, no matter how they arrive to the stakeholder. Common signs of social engineering should be taught, especially of the popular threats arriving via email and from websites, but also of those emanating from social media, instant messaging, SMS, and voice calls.

Social Engineering Red Flags PDF

KnowBe4 offers a Social Engineering Red Flags PDF document, shown below, which lists 22 different signs that anyone can use to investigate an incoming email to determine if it is a potential phishing email. It includes commonsense signs we should notice as dubious when we open an email. Things like potentially dangerous attachments, grammar issues indicating the sender is not a native language speaker, an unusual request, sent at a strange time, etc. The PDF puts almost two dozen common "red flags" all in one place. It's a quick, easy read that reinforcements several key signs that might indicate a suspicious email. It is made to share with stakeholders.

All employees need to be taught how to recognize the signs of social engineering and phishing.



You can also read the related Red Flags of Social Engineering article: https://blog.knowbe4.com/share-the-red-flags-of-social-engineering-infographic-with-your-employees

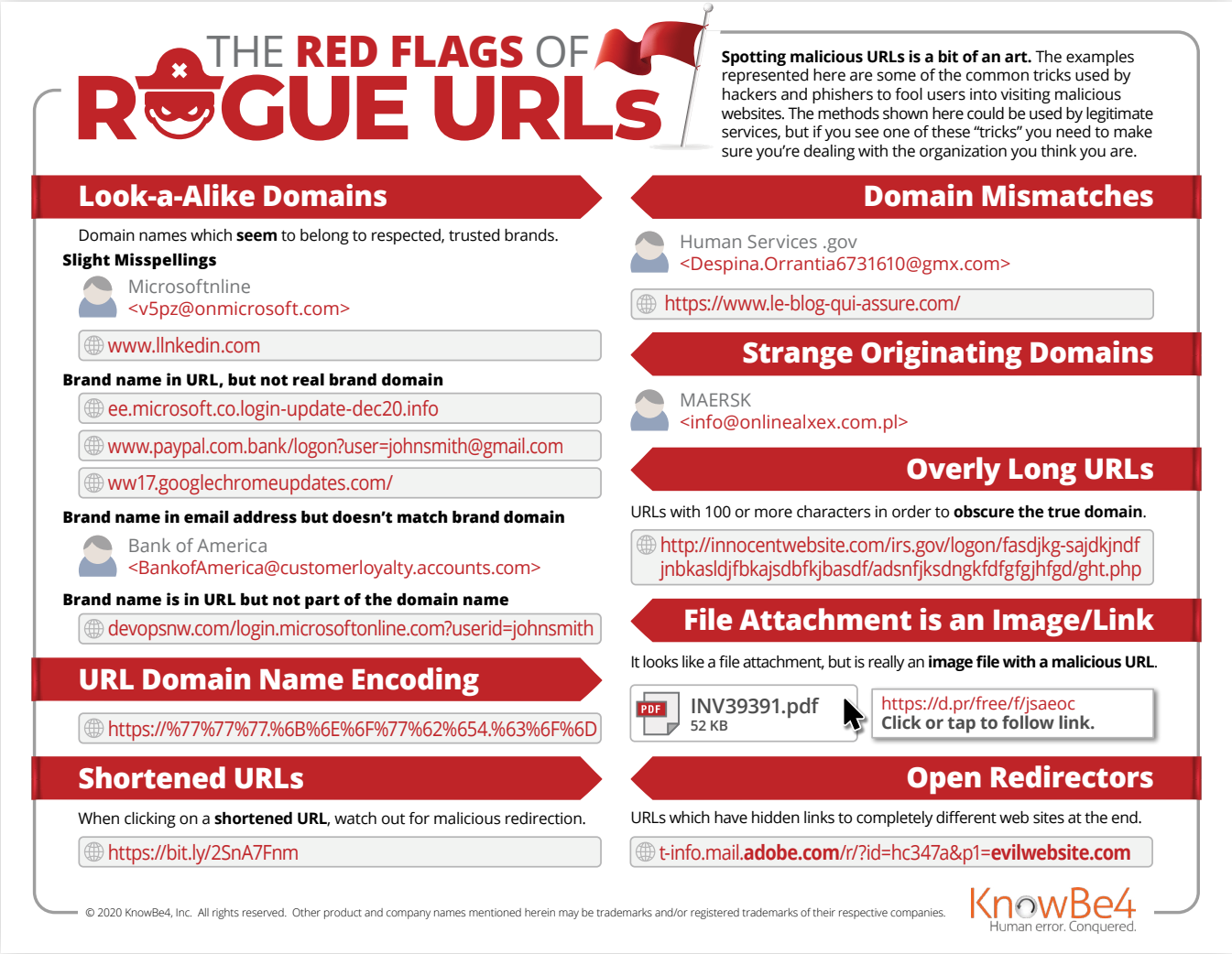
For readers and admins with more interest in learning how to better forensically determine if a suspicious-looking email is malicious or not, KnowBe4 offers a 1-hour webinar entitled CyberCSI: Forensically Examining Emails (https://info.knowbe4.com/phishing-forensics). It covers visual clues, email header inspection, research, and tools to help anyone better determine if an email is malicious or not.

Recognizing Rogue URLs

After recognizing common red flags of email social engineering, the next best skill to communicate is how to recognize rogue URL (uniform resource locator) paths, which will often be displayed in an email or located on a website. Phishers love to use dozens of tricks to fool unsuspecting potential victims into clicking on their malicious URL.

Red Flags of Rogue URL PDFs

KnowBe4 created another PDF document, shown below, which shares many of the most common signs of rogue URLs. It is designed to be shared with stakeholders.



KnowBe4 also offers a one-hour-long related webinar on how to spot rogue URLs: https://info.knowbe4.com/rogue-urls

Alternately, you can read a related blog article on the same topic: https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks

All employees need to be taught the signs of malicious URLs.

What To Do When a Phish Is Detected

After teaching stakeholders how to recognize a social engineering attack, it is nearly as important to teach them what to do next. Policy needs to dictate to stakeholders the actions they need to take to best protect the organization. It's not enough for a targeted victim just to ignore or delete a phishing attack. All phishing attacks should be reported to a central collection point or email. Instead, all stakeholders should be taught to report a suspected or confirmed phishing attack to a previously communicated contact point, before deleting or forwarding the phishing example.

It's important that all users be taught what to do when a phishing attack is suspected. It's not enough just to ignore or delete.

It's always best if all suspected or confirmed phishing attacks can be collected to a centralized aggregation point so that the attacks can be noted, confirmed, tracked, trended, reported on, and responded to. Without consistent reporting of phishing attacks, a single reported attack cannot be distinguished between a rare one-off to a single individual never to be repeated again; and a sustained attack to multiple individuals as part of a coordinated phishing campaign with a common objective.

A Fortune 10 CISO once lamented that it wasn't until the 900th targeted person in his organization had reported a phishing attack, was his IT security team able to analyze and confirm thousands of targeted employees with hundreds of stolen login credentials sent to the attacker from a week-long sustained phishing campaign. The CISO wondered what would have happened to his organization had the 900th person not decided to report it?

It's also important to reiterate to stakeholders that they should report any actions they took with a suspicious phishing attack which could have let the phishing attack be successful. For example, if a potential victim was tricked into providing login credentials or into running suspicious software, the victim should always be encouraged to report their actions without fear of additional repercussions. You want to communicate that it is "safe" to report potentially risky behavior; which is safer than letting it go unreported. You do not want to create an unhealthy culture where potential victims are fearful of reprisals and are "taught" to not report potential threats. Silence increases risk.

Users should be taught to report suspected phishing attacks.

Phish Alert Button

The best anti-phishing programs give users an easy way to report suspected phishes. KnowBe4 offers a free Phish Alert Button program. It can be downloaded here: https://www.knowbe4.com/free-phish-alert

The Phish Alert Button program installs an icon (shown below) into Microsoft Outlook and Google Gmail email client, which can be clicked by a potential victim when they suspect a potential phishing email. When installed, the Phish Alert Button is configured to delete and forward all selected potential phishing emails to a common email address. Administrators should configure the button to forward all sent suspected phishing emails to a desired central aggregation email address, where the phishing reports can be analyzed, confirmed, researched, and trended.

The Phish Alert Button functionality can be modified by additional backend processes or features, such as KnowBe4's PhishER to notify end users of whether the reported, suspected phishing email was truly a malicious email, test, or something less innocuous like a spam. Replying to the end user with a confirmed analysis provides a feedback loop, which further encourages the user to report future suspected phishing emails.

Regardless of the tool used, administrators should strive to make reporting suspected phishing easy and quick.

Other Common Example Policies

Here are some other common anti-phishing policy examples that anyone should consider adding to their security policies:

"Be suspicious of emails asking for your login credentials to validate them or asking you to log in to validate a supposedly detected security event."

"Users should "hover" over all URL links or otherwise verify that they appear to come from legitimate, trustworthy domains before clicking on the link. When in doubt, ask a more knowledgeable IT person to analyze and confirm."

"Don't install unauthorized software."

"Never give your login credentials in request to an email or link sent inside of an email, unless you know for sure the request is valid, from the legitimate sender, and is expected."

"Always be suspicious of emails arriving from unexpected senders."

"Always verify the email address of the sender of any received email. Be suspicious of any email claiming to be from a previously trusted sender that arrives from a previously unknown email address."

"Treat all unexpected file attachments as potentially suspicious. Call the sender at a predefined phone

number to verify if he/she intended to send the included file attachment before opening."

"Never allow scripts, macros, or other "active content" to run when opening a file attachment from an email."

"When in doubt about an email or unexpected request in an email, call the sender at a predefined phone number."

"Never install software offered by a third-party website. If you are told a particular type or version of software is needed, always visit the official vendor's website to install the software."

Preventing Business Email Compromise Scams

Business Email Compromise (BEC) phishing scams are costing businesses billions of dollars a year (https://blog.knowbe4.com/the-fbi-updates-their-numbers-and-bec-is-now-a-26-billion-dollar-scam). A BEC scam usually arrives as an email pretending to arrive from a trusted person asking for a new invoice to be paid or for ongoing, regular payments to be made to a new destination. The unsuspecting victim(s) pay the fraudulent invoice or send an otherwise routine payment to a fraudulent destination, where the money is then stolen by the perpetrator. Oftentimes, the request appears to come from a supervisor, senior executive, or mission-critical vendor, who claims they are currently uncontactable (e.g., flying, on an important business trip, cell phone not working, etc.), along with a claim that the payment must be made immediately or an important business transaction will not occur.

BEC scams can be mitigated by creating a policy that requires that all new requests for new payments or payment destination changes be confirmed by calling the requestor on a previously verified phone number to corroborate the request. The policy must ironclad and supported by senior management so that no employee feels pressured to make an unexpected, "last minute" payment or change without the required verification.

You can read more about BEC scams and mitigations in this KnowBe4 white paper:
https://info.knowbe4.com/ceo-fraud-prevention-manual

Notice of Training and Methods

It is important to clearly communicate to all stakeholders the importance of security awareness training and how it is accomplished. In the past, some implementers believed that administrators should be opaque about the use of simulated phishing tests as part of the educational process—they believed that tested recipients should be "surprised", like they would be with a real-world attempted phishing exploit. But these "surprises" were often not met with congratulations or approval, especially by senior management. It was determined that making stakeholders aware of security awareness training and the use of simulated phishing tests did not dimmish their value or the likelihood that a potential tested stakeholder would or would not be fooled by a particular simulated phishing campaign. Indeed, letting stakeholders know of training and the accompanying simulated phishing campaigns is now considered a crucial part of the overall education. Letting stakeholders know they will be tested brings heightened awareness, which will benefit the testing organization's results.

All stakeholders should be made aware of security awareness training, how it is accomplished, general frequency, and what tools and methods will be used. It's important to communicate how training is accomplished, so that participants will not fall for fraudulent phishing scams appearing as "required training" from the organization or the organization's selected security awareness training vendor. Scammers often try to use an organization's selected and well-known security awareness training vendor's brand as a way to get employees to click on fraudulent emails.

It's important to consider the tone of related communications. The organization should approach this notification as an opportunity to build the right relationship with stakeholders up front. Let them know that you aren't testing them to punish them, laugh at them, etc... Instead, this is something that everyone needs to be exposed to so that the overall risk to the organization can be reduced.

Here is an example policy statement:

> *"This organization proactively fights using the best combination of policy, technical defenses, and training to prevent cybersecurity incidents. As part of those defenses, we require all employees to take security awareness training. All employees take this training upon hiring and then at least monthly thereafter. Training can come in many forms, including: emails, training videos, posters, and games. As part of the training, we send bi-weekly simulated phishing tests to gauge the effectiveness of that training and to allow us to know when and where additional training might be beneficial. This organization uses KnowBe4 as its primary security awareness training vendor. You should expect monthly requests to take training, which may or may not include quizzes to rank an employee's understanding of the material. You can go to https://www.[???].com/SAT to see what training you have taken and are required to take at this time. Send any questions you may have to SAT@company.com."*

Consequences for Failed Tests or Real Exploitation

Most organizations think there is value in implementing consequences for stakeholders failing simulated phishing tests or for falling for real phishing attacks. They believe that having negative consequences helps to reinforce the training and caring. Consequences can range from additional training and/or testing, counseling, restriction of duties, and even separation of employment. To be clear, KnowBe4 believes in "more honey and less sticks". Anyone...anyone...can be fooled by the social engineering and phishing, depending on the angle, timing, and environment. It is difficult to impossible to prevent any person from falling for a real-world or simulated phishing test. This is not to say that appropriate consequences don't have their value. Consequences that organizations have used include:

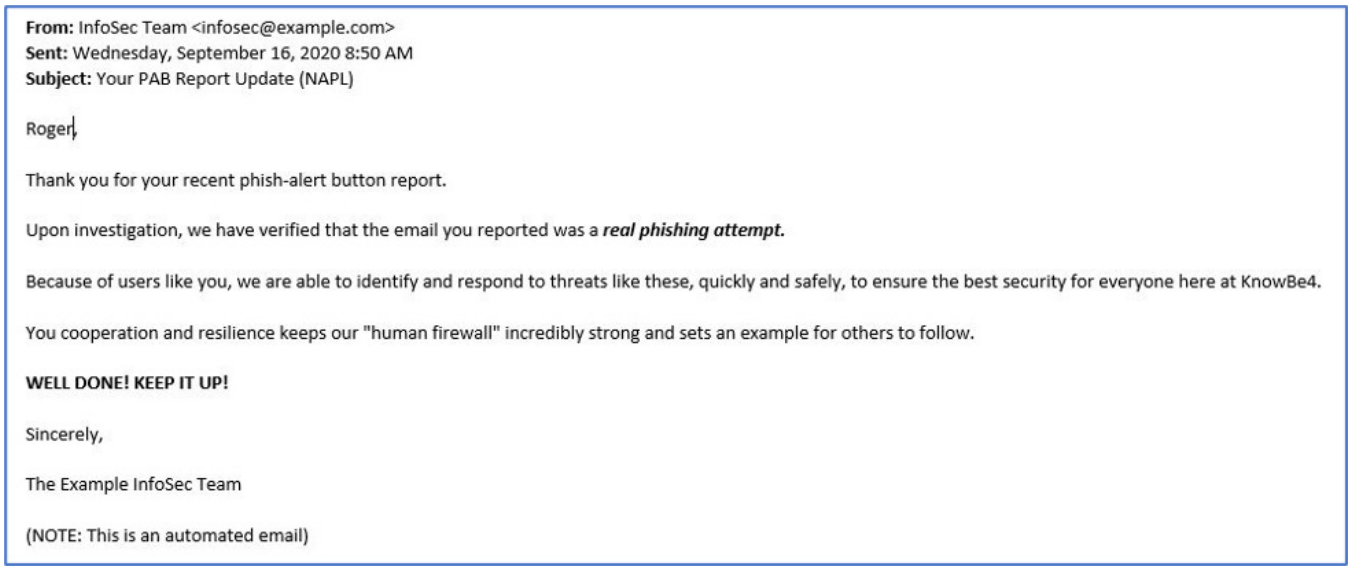
- Additional education and training
- Escalating education and training, increasing with a growing number of failures
- Locking down a user's workstation or device in a way to reduce risk from a successful exploitation
- Counseling from a stakeholder's supervisor
- Forced password changes (to reduce risk from a real phish in the past may have been successful)
- Attendance at longer, in-person training
- Creation of a resolution/correction plan by stakeholder and his/her supervisor to help gain success
- Involvement of Human Resources

- Inclusion in annual review
- Reduction of bonus or salary
- Separation of employment

Whatever consequences are possible should be clearly communicated to all stakeholders. Each type of possible consequence should be defined, including what it takes to get a specific consequence. Consequences and how they are earned should not be surprises. Consequences should be applied equally across the organization so that senior management gets treated the same as front-line employees. You want everyone to see that computer security is an important, and equal, part of everyone's job with identical consequences.

Positive Reinforcement

KnowBe4 believes in primarily driving anti-phishing behaviors by positive reinforcement. This can include simple email feedback "rewards" for an employee successfully reporting a real-world phish or simulated phishing test. An example is shown below.



From: InfoSec Team <infosec@example.com>
Sent: Wednesday, September 16, 2020 8:50 AM
Subject: Your PAB Report Update (NAPL)

Roger,

Thank you for your recent phish-alert button report.

Upon investigation, we have verified that the email you reported was a ***real phishing attempt.***

Because of users like you, we are able to identify and respond to threats like these, quickly and safely, to ensure the best security for everyone here at KnowBe4.

You cooperation and resilience keeps our "human firewall" incredibly strong and sets an example for others to follow.

WELL DONE! KEEP IT UP!

Sincerely,

The Example InfoSec Team

(NOTE: This is an automated email)

Positive reinforcements can include special public recognition, small gifts, gift certificates, department pizza parties, and even additional cash bonuses.

One employer stated that he rewarded any employee not falling for a single real world or simulated phishing attack with a $1000 bonus at the end of the year. When asked how he could justify such a large expense for an employee simply following required security policy, he replied, "Considering how often phishing is involved with data breaches and how well my employees now deal with phishing, I consider it the best money I spend on IT security. It's cheap compared to what it would cost my business if a single phishing attack was successful."

There is no one "right" set of consequences and positive reinforcement that works for all organizations. The actions involved are based on the type of organization, its own risk tolerances, its starting "Phish-Prone™" baseline, and what actions will best help to drive the right behaviors most quickly and consistently. The end goal is to help the entire organization's culture care about preventing social engineering and phishing, however that is accomplished. Organizations should attempt to

find the right combination of consequences and positive reinforcement actions that work best for them and their stakeholders.

Employee Monitoring

Stakeholder privacy must be considered when implementing a security awareness training plan, especially if a stakeholder's email, other communications, and actions, are monitored as part of that program. Sometimes, something as simple as tracking which simulated phishing tests a stakeholder passed or failed may require permission or notice. When permission is required and/or what notices need to be made depend on the organization's legal and regulation requirements. Every organization should consult with their legal department to determine what declarations need to be made to be compliant with laws and regulations.

Incident Response

It must be decided on ahead of time, and documented in policy, and with related incident response employees, how an organization will respond to a particular successful phishing event (or multiple, coordinated, failed phishing attempts). You don't want to be making decisions after the fact or during the possible stress of a successful exploitation. You need to decide ahead of time what phishing events will require a formal incident response. For example, can just a single, successful, phishing event cause an official incident response or does it take a sustained, coordinated phishing campaign against many employees, even if not yet successful, result in a formal response? How will a successful exploitation be handled? How are leaked credentials responded to? How will the execution of a malicious program be handled, and so on?

If you are going to use an outside vendor as part of your incident response plan during a crisis event, the time to call and introduce yourself is before a crisis is in progress. Simply calling and saying hello to the contact person and asking what to expect can significantly improve the overall experience if a cybersecurity crisis ever develops.

Hint: If you are worried about legal implications of a cybersecurity event, have your lawyer make any external contacts (email, phone, etc.) to other external vendors, that way the communications become "privileged communications" and are harder to be requested and used against you in court.

Part of incident response to a successful real-world exploitation is the question of whether a preventative or detective control needs to created or be updated to help mitigate the next similar event. Do policies need updating? Does training need to be updated? Was the bypass a one-off or rare mistake or does something systematic need to change to prevent the next occurrence?

Incident Response must be coordinated, planned, and communicated to everyone involved. This topic is too broad to summarize in this document. All organizations are encouraged to develop formal incident response plans. Those plans should include phishing and social engineering exploitations in their use cases.

Other Policies To Consider

Here are some other related issues or policies to consider:

MFA Use

Multifactor authentication (MFA) can significantly reduce some forms of social engineering and phishing. You can't get phished out of a password if you don't have one. With that said, no single MFA solution works with all needed authentication-requiring sites and services. All stakeholders will be using a combination of passwords, and optionally, MFA (one or more types), for years to come.

It is important that anyone using MFA be aware of what risks MFA mitigates and which they do not. Any stakeholder using MFA should be educated about what types of attacks, including phishing and social engineering, can bypass or hack their particular MFA solution.

How MFA can be hacked and what mitigations and education should be included with any MFA solution can be learned from the following resources:

12 Ways to Hack MFA webinar: https://info.knowbe4.com/webinar-12-ways-to-defeat-mfa

Free, 41-page Hacking MFA ebook: https://info.knowbe4.com/12-way-to-hack-two-factor-authentication

Free, Multifactor Authentication Security Assessment tool:
https://www.knowbe4.com/multi-factor-authentication-security-assessment

KnowBe4's Multifactor Authentication web portal:
https://www.knowbe4.com/how-to-hack-multi-factor-authentication

Hacking Multifactor Authentication book (Wiley):
https://www.amazon.com/Hacking-Multifactor-Authentication-Roger-Grimes/dp/1119650798

Ransom Payment Policy—Pay or Not Pay?

An organization should decide ahead of time if they are willing to pay a ransom because of a ransomware event. Having to decide on the spot during the damage and stress of an active ransomware event is probably not the time to decide. Some organizations decide it's unethical to even pay a ransom and others are worried about the potential legal repercussions.

The first thing any organization should decide is if they truly have a good, verified backup of all critical systems that can be confidentially restored in an acceptable time frame should their files and servers become unavailable. Most organizations believe they have this, but many do not. They have never tested their backups at a scale that a single ransomware event can cause. Additionally, many good, tested backups have been corrupted by ransomware actions, turning what was believed to be a rock-solid recovery plan into a crisis where no other good action besides paying the ransom can easily alleviate the situation. Additionally, ransomware routinely now does other things, such as:

- Exfiltrating critical and confidential data and emails and threatening to release it publicly, to hackers, and to competitors, unless the ransom is paid
- Stealing professional and personal employee credentials and threatening and ransoming employees
- Stealing customer credentials, if available, and threatening and ransoming customers
- Using a victim's network and email system to send trusted third-party spear phishing emails to people and organizations with which the victim does business
- Publicly shaming compromised victims on blogs, social media, and websites

Over half of all ransomware exploitations now involve these additional actions, and the percentage of ransomware that is using these actions is increasing over time. None of these five actions being accomplished by ransomware gangs can be prevented by a good backup and restore process. All of them can result in substantial financial and reputational damage, which is not easy to repair. Senior management should be told of these new ransomware actions when deciding if they will or won't pay the ransom if a significant ransomware exploit occurs within the organization.

Learn more about the new actions of ransomware by watching this one-hour long KnowBe4 webinar:
https://info.knowbe4.com/nuclear-ransomware

Learn about ransomware and what you can do to defend yourself by reading KnowBe4's Ransomware Hostage Rescue Manual: https://info.knowbe4.com/ransomware-hostage-rescue-manual-0

You can read and learn more about ransomware here: https://www.knowbe4.com/ransomware

Crisis Management

Social engineering and phishing attacks can inflict significant damage on an organization. Every firm should decide if it makes sense to hire or discuss potential future work with a crisis management firm if the worst case scenario happens. Crisis management consultants specialize in helping to contain the spread of damage and work on a public relations plan to help best communicate with customers, employees, and the external world.

Disaster Recovery Plan/Business Continuity Plan

Most firms hit by significant ransomware attacks have significant business interruption for at least week, and sometimes months. Every organization should already have both a disaster recovery plan and a business continuity plan to help minimize damage during a cybersecurity event crisis.

Cybersecurity Insurance

All organizations should investigate paying for cybersecurity insurance. Cybersecurity insurance helps to limit financial damage from a covered cybersecurity incident to the maximum of the agreed upon deductible. Just as important, when a customer calls the insurance company for a covered event, the insurance company will usually put the victim in contact with an expert incident response vendor. These vendors normally have extensive experience in minimizing the damage from a cybersecurity event and in the quickest reasonable recovery for the victim. The cybersecurity insurance company uses this incident response vendor because they do a good job at minimizing damages and enabling quick recovery. Although the cost of cybersecurity insurance has been rising over time recently (due to payouts involving ransomware attacks), it still ranks as one of the best coverages for the risk covered and the money spent on premiums.

Note: KnowBe4's KCM GRC Platform product helps organizations write policies and controls and track compliance. The KCM GRC Platform is offered in different packages to meet the needs of all organizations and is available with the following modules to choose from:

- Compliance Management
- Policy Management
- Risk Management
- Vendor Risk Management

Streamline your compliance, risk, and audit management with KCM GRC.

Policy Summary

Every organization should create the best policies possible to fight social engineering and phishing. Hopefully, the examples covered above will help you craft the best policies possible. Ultimately, a specific anti-phishing policy should communicate education and actions which best protect the organization against social engineering and phishing exploitation, hopefully communicating a healthy, appropriate level of skepticism as part of the organizational culture. The policies should help mitigate the risks and damages from social engineering and phishing, and instruct all stakeholders to take appropriate actions should they be involved in an attempted or successful phishing attack.

TECHNICAL DEFENSES TO FIGHT SOCIAL ENGINEERING AND PHISHING

This section summarizes the technical defenses that any organization should have to effectively fight social engineering and phishing. While it is impossible for any single document to cover every single possible defense, this ebook attempts to summarize the most popular options to consider.

Defense-in-Depth

Before we discuss technical defenses, the concept of "defense-in-depth" must be discussed. Defense-in-depth is an IT security concept which believes that any single computer security event mitigation will not be perfect and is subject to unexpected failure. Because of this, defenders should implement multiple, overlapping defenses which help to ensure that what one mitigation misses, another may catch. Relying on only one mitigation for your defense is a high-risk decision.

Where Technical Defenses Should Be Located

There is a fundamental decision of where a cybersecurity defense should be located. Following the defense-in-depth concept, computer defenses should be located everywhere: on the network edge, between networks, on ingress points, on egress points, on individual hosts and devices, and in the cloud. Many defenses work best located in a particular location and others work best in multiple locations. In general, most defenses inspect and analyze inbound network traffic and newly occurring software, events, and actions. Technical defenses can be in place working all the time or just be called "on-the-fly" when requested by an administrator or user.

Network Security Boundaries

A core belief of many security defenders is the idea of dropping unwanted or unnecessary network traffic and/or connections. Doing so decreases the chance of successful exploitation unless the adversaries learn and/or abuse allowed traffic flows. Network routers do the bulk of network separation on the Internet and between internal networks. Routers typically define network security boundaries by physical locations and logical (IP) addresses.

Firewalls often allow or block network traffic based on IP addresses, ports, and other network packet data characteristics (such as network packet flags or application data). Firewalls are often installed at network perimeters, but are also commonly installed on host computers and devices. For example, Microsoft has included a built-in, default-enabled firewall on Microsoft Windows since it released Windows XP Service Pack 2 (in 2004). Apple and Unix/Linux-style operating systems have long included host-based firewalls, but they usually aren't enabled by default. Firewalls can often define rules based on users, groups, services, and applications. Application-level firewalls can help prevent previously known malicious traffic and even unknown traffic malformations from abusing an application or service. Virtual Local Area Networks (vLANs) and Software-Defined Networks are often used to create logical network boundaries on internal networks and within virtual machine networks.

With this said, most network security boundary devices have limited impact on preventing social engineering and phishing, because these attacks occur over very common, allowed network pathways (e.g., HTTP, SMTP, etc.) and its discussion is included here mostly for inclusivity. However, if a firewall can do content inspection, it may be able to prevent phishing and social engineering attacks from reaching a user.

Content Filtering

One of the best ways to prevent social engineering and phishing is for the involved network pathways or application data to be inspected for malicious-looking patterns. Content-filtering services abound from multiple vendors covering multiple locations. Most major email services include built-in content filtering. Most browsers, which often function as host HTTP-enabled email clients, also do content filtering. Network perimeter devices, intrusion detection devices, antivirus inspection services (both host and network), and email servers, often do content filtering. Content-filtering services, looking to block spam and phishing content are often the primary and best technical methods to mitigate phishing threats. However, even the best content filters, even layered in the best defense-in-depth strategy are going to allow some malware and phishing content to get by to the user. This is just a fact of life. But, yes, by all means, enable the best, layered content filtering that you can. It can only help to mitigate a substantial part of the risk. Occasionally, when tuned too aggressively, content-filtering services can inappropriately block legitimate content. All content filters need to be tuned to block as much real, malicious content as possible without incurring any false-positives and blocking legitimate content.

Identification Services

Many anti-phishing software programs and services can automatically identify phishing, spam, and other types of related threats, and either block them from reaching the end user at all, quarantine the identified content for further expert analysis and treatment, or pass along to the end user with additional label appended to the subject text (i.e. [SPAM], [LIKELY PHISHING], [THREAT], etc.).

KnowBe4 offers a related tool called PhishER™ (https://www.knowbe4.com/products/phisher). It helps to quickly identify email threats, and allows administrators to review, approve, and identify threats, either manually or using rules and automatic. PhishER is a tool which allows faster anti-phishing analysis and outcomes. Administrator can also click on any individually reported email and tell PhishER to go out and immediately remove similar messages from everyone's inbox. Rules and artificial intelligence can be used to automate some or all of the actions. Either way, PhishER, and other tools like it, helps to quickly collect, identify, and treat dangerous threats.

Detonation Sandboxes

A relatively new technical solution, detonation sandboxes, are devices or software which intercept potentially malicious content—mostly file attachments and Internet content from clicked URLs. They temporarily block or prevent them from executing in the user's current security context so they can do no harm. They then open them in a variety of virtual environments which attempt to realistically mimic the core components of a device's existing environment where the blocked content would have otherwise executed or opened. The content and the outcome of executed content in the alternative, safe location (i.e., the "sandbox") is then analyzed to help determine safety and legitimacy versus potential malicious outcomes. If the content is deemed safe, it is then allowed to execute on the user's device in the original, intended manner.

Many vendors offer robust, sophisticated solutions. Oftentimes, all the user notices is a slight delay, perhaps a second or three, before the content is allowed to execute as the user desired. Other solutions will rewrite URL paths, replacing it with safer alternatives that the user will notice if he/she is paying attention. Many security experts decry the URL re-writing, as the modified path renaming makes it difficult to impossible for a knowledgeable user to analyze for maliciousness using their own expertise as they could have with the original, untainted URL. Detonation sandboxes have gained widespread use, but are still not as ubiquitous as other types of more common defenses, such as firewalls and content filters. As grand as they claim to be, they will sometimes fail to recognize and block malicious content, although they tend to have more accuracy than antivirus software.

Note: Many antivirus programs contain and work using internal detonation sandboxes to help them analyze potential malware.

Reputation Services

Reputation services will advise, block, or allow content based upon its origination URL pathway, domain name, or IP address. The earliest (and still popularly used) reputation services were crude **blacklisting** services which contained lists of domains previously reported as malicious. These lists or databases could be downloaded or referenced by other services, such as email servers or browsers, to help allow or deny content. Early, popular blacklisting services include: Spamhaus, DNSBL, Ospam, and Google Safe Browsing. Another, known as the Blacklist Master, contains pointers to over a 100 individual blacklists.

Note: The opposite of a blacklist is a **whitelist**, where only content coming from previously verified and allowed domains, can be loaded.

Some organizations will deny all content and network traffic originating from entire countries (such as Russia or China) using IP addresses, Border Gateway Protocol assigned number addresses (which help route traffic on the Internet), or high-level domain names assigned to countries (such as .ru and .ch). These are the crudest types of blacklists, denying or allowing all traffic and content from a whole country, throwing the good out with the bad in wholesale fashion. Still, some organizations, without any business in particular countries with an overabundance of malicious content, find it an acceptable, even if brutish, solution.

Another related, far less popular alternative solution is called greylisting. **Greylisting** services typically block all incoming emails or content coming from any sender or domain not previously approved (like a whitelisting service would). But the greylisting service will use a method to then confirm the legitimacy of the previously unrecognized email address or domain. If implemented on an email server, the greylisting service may ask the denied transmitting email server to retry again at a later time or date. Legitimate email servers often will, but rogue email services often used by spammers and phishers, will not (as they are usually far less sophisticated than a real email server). Greylisting can crudely stop some bad emails and content, but they also tend to have a higher than acceptable rate of rejecting legitimate emails and wanted content. Users often complain because they never receive legitimate emails and may only much later learn of the rejection when the sender complains verbally of the non-response to a question or desired action.

Many vendors offer sophisticated reputation services which use frequently updated dynamic whitelists and blacklists as a starting point, but adding content-filtering, and dynamic, “intelligent” rules, and machine learning engines which inspect dozens to hundreds of attributes to determine intent. Many times, users can submit new links and content for inspection and the resulting reputation check puts the content or link on a permanent blacklist or whitelist.

In all implementation types, crude or sophisticated, it is possible for legitimate content and URLs to be incorrectly flagged as malicious. And it can often take extraordinary effort to get a wrongly listed piece of content or URL delisted. It is not even uncommon for it to be impossible to get a mistake corrected and wrongly maligned parties are forced to accept the wrong decision of another party which has some control over who does and doesn’t get to see their legitimate content or domain. These permanent mistakes are seen as a “growing pain” in an attempt to protect Internet users. After decades of use, the wrongs of reputation services do not seem to be getting significantly better. Still, there is hope that some day their incidences of false-positives and false-negatives will diminish.

DNS Checks

Some parties have noticed that phishing emails often (but not always) come from newly created domains. So, they will create services or scripts that will analyze the domain name of an incoming email or Internet URL and block those which seem strangely young or contain other highly suspicious behavior (such as originating from a dynamic DNS service). These types of DNS checks do a good job at blocking malicious content originating from anomalous domains, with a fairly low incidence of wrongly blocking legitimate content, but a large portion of phishing attacks originates from legitimate and long-established domains. For example, phishers often use Google's Gmail email service to create fraudulent email addresses. Google's gmail.com domain is one of the most famous and legitimate domains possible, and as such, any phishing emails originating from it would not be blocked.

Malware Mitigation

It goes without saying that traditional malware mitigation services, widely and traditionally known as antivirus (AV), can detect and prevent malicious URLs, content, and file attachments. More sophisticated versions, known as Endpoint Detection & Response (EDR), are becoming more popular; although their differences are sometimes hard to define.

Although AV/EDR vendors often self-report very high rates of accuracy (100% is often claimed), their ability to detect and block the millions of new malware programs created every week challenges those claims. Malware creators often monitor Google's Virustotal (https://virustotal.com) service, which runs over 70 different AV/EDR engines in order to see when their malicious creation starts to get identified. When this happens, the malware program will update itself to a new, less detected variant. Using this method, a malware program can go days to months without reliable, widespread AV/EDR detection. This is further evidenced by the fact that most organizations with malware-compromised environments had widespread, up to date, AV/EDR.

Note: Many ransomware programs exist for months to over a year in the compromised environment, without any detection, before they execute their malicious behavior.

With this large problem of accuracy looming over them, like firewalls, most organizations still feel obligated to run AV/EDR. Even if they don't always catch malware, whatever they do to detect and block is a win for the protected environment.

Deploy a Tool for Easy Reporting

As covered above, making it easy for stakeholders to report suspected phishing can greatly improve the success of any anti-phishing program. Consider using KnowBe4's Phish Alert Button. It works with Google Gmail and Microsoft Outook.

Implement Least Privilege Permissions

Another core defense practiced by every computer security practitioner is that of least privilege permissions. The least privilege permissions concept says the bare minimum security permissions needed to accomplish a task should always be assigned to a security principal (i.e., user, computer, device, group, service, daemon, network, etc.), so that any abuse of that security principal's security context, either by the principal themselves or some other malicious actor in the principal's security context can do the least amount of harm.

Hackers and malware, including socially engineered Trojan Horse programs, always want to operate in the highest security context possible. If they can get access to a user's desktop or programs, at the very least they get the security context (and whatever privileges and permissions) the user has. If they can access or take over an elevated program or service, they can get the security access of the program or service. For example, a buffer overflowed program allows the attacker or malware to take over the security context of the buffer overflowed program. So, if a Windows service is running in the Local System security context, then the malware or attacker will get the security context of the all-powerful Local System built-in account.

If an attacker or malware doesn't get an elevated level of security context during the initial stages of their attack, they will often try to do secondary "escalation of privilege" (EoP) attacks to get elevated access, but an EOP attack method is not always guaranteed to be available or successful. Administrators and users can often complicate hacker and malware malicious attempts by not letting them get elevated access. One of the best ways to do that is for users, administrators, programs, services, etc., to not be running in elevated security contexts where they can be overtaken by hackers and malware (i.e., least privilege).

To accomplish that, all organizations to try to implement least privileged permissions as a core defense and practice everywhere they can. Practicing least privilege permissions includes:

- Give the least level of permissions and privileges necessary to a security principal (e.g., user, group, service, etc.) needed to do their assigned active task
- Don't allow administrators or users to be logged in with elevated security contexts while performing tasks not needing elevated access (e.g., browsing the Internet, doing email, using word processing programs, etc.)
- Minimize the number of permanent members of any elevated group (e.g., Administrators, root, Domain Admins, Enterprise Admins, etc.)
- Require admins to "check-out" privileged accounts when needed, and time-limit the ability for the account's use
- Protect elevated logins using multifactor authentication or other elevated authentication mechanisms if possible
- Passwords for elevated security context accounts should always be long and complex (at least 16 characters) and changed at least annually
- Elevated accounts should be heavily monitored for appropriate use
- Elevated groups should be periodically audited to remove unneeded permanent members
- Accounts with elevated security contexts should be periodically audited to ensure they are still needed and used
- Elevated security context should be used sparingly on less trusted devices and workstations

The concept of least privilege permissions is one that all organizations should follow and apply whenever possible. Doing so will decrease the chances that hackers or malware will be successful and reduce overall cybersecurity; helping you far beyond just reducing social engineering and phishing success.

Email Client Protections

Today, most email clients come with strongly configured, default security settings, including many anti-phishing features. For example, most email clients will not automatically download externally linked content when an email is opened or allow a potentially malicious file attachment to be immediately opened. Instead, it will display placeholders and prompt the user to click on an additional button to download the potentially malicious content or file attachments. Most of the time, the best protection that an admin or a user can implement is not to weaken the already strong and secure security settings enabled by default.

Browser Protections

Like most email clients, most browser clients have strong, default security settings. Internet browsers have been popular attack targets for decades. Those attacks have forced browsers to become extraordinarily strong at defeating known attacks. Most of the major browsers include content filtering, reputation services, and almost an obnoxious number of warning prompts if a user goes to download or execute potentially malicious content.

With that said, browsers routinely get dozens of found bugs patched each month. This means browsers are always full of readily exploitable vulnerabilities. Malware writers and phishers are constantly looking for, finding, and exploiting newly discovered vulnerabilities. It is truly a war of constant attrition between the browser vendors and malicious actors, and the browser vendors are often playing catch up. But like email clients, the best thing most admins and users can do is to keep their browser patched and up to date and not weaken the already fairly strong security configuration settings.

Implement Global Phishing Protection Standards

There are three global email security standards you should be using: **Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM),** and **Domain-Based Message Authentication, Reporting, and Conformance (DMARC)**. If you are not using them, you should be. They've been around for many years and used and trusted by millions of people. They can only help.

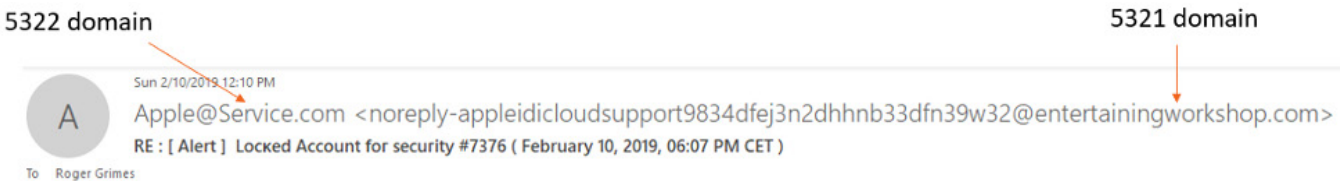
SPF, DKIM, and DMARC allow organizations to prevent malicious third parties from spoofing the organization's legitimate email domains to others who might rely on it. They don't work perfectly, but when enabled, will cut down on some forms of email maliciousness.

All three work by the sender's email domain administrator enabling them in DNS using TXT records (or alternately, enabling it in their email host provider's administrative console). When enabled, receivers (actually, their email servers or clients on their behalf) of emails from activated domains can check additional information to verify whether or not a particular email actually came from the email domain it is claiming it was sent from.

Sending domains enable these protocols so that receivers can verify that emails which claim to be from the sender's domain really are from the sender's domain. Senders enable it so other people can't claim to be them. And receivers enable it so they can verify whether or not a particular email really is from where it says it's from. It takes both sides to be enabled to work. Enabling them can't hurt anything, unless you decide to take the draconian step of rejecting all emails which fail any of the checks. Hint: This will cause far too many false positives, so choose to quarantine instead.

SPF works by preventing spoofing of an email's real return email address (i.e., the email address that you would be sending a reply to) domain. This email address is known as the 5321 address (because it is defined in RFC 5321, which defines Simple Mail Transfer Protocol). Depending on the email client, the 5321 address may not always be displayed. This is especially true of small form-factor email clients, such as the ones you see on smartphones.

DKIM works by preventing the spoofing of the "Display From" email address (from RFC 5322, Internet Message Form email standard) domain. The Display From address is almost always shown to an end user when he/she previews or opens an email, hence its name. The figure below shows the difference between the 5321 and 5322 email addresses.



Although these addresses can be different even in legitimate emails, they are more likely to be different in malicious emails. SPF and DKIM work to allow receivers of emails to ensure that the domains (and domains only) of a received email are really from the email servers of those claimed domains. However, they do it quite differently. DMARC is an additional standard that essentially tells others relying on your SPF and DKIM records how they should treat failing/spoofed emails.

Note: It's important to note that SPF and DKIM only verify the legitimacy of the sending and claimed domains (e.g., @example.com). The email address name portion before the email domain (e.g., roger@ or rogerg@) could still be spoofed by a malicious sender.

Using SPF

SPF works by allowing receivers to verify that the senders claimed email domain (the 5321 address domain) really comes from the authorized email servers (by IP address) of that domain. Senders enable this for their domain by creating at least one DNS TXT record. When creating the SPF DNS TXT record, you need to have a few pieces of information handy, and these include: which email server(s) do you want handling each defined domain and what are their public IP addresses.

Useful SPF configuration links include:
https://support.rackspace.com/how-to/create-an-spf-txt-record/
https://www.validity.com/how-to-build-your-spf-record-in-5-simple-steps/
https://stopemailfraud.proofpoint.com/spf/
https://www.spfwizard.com/

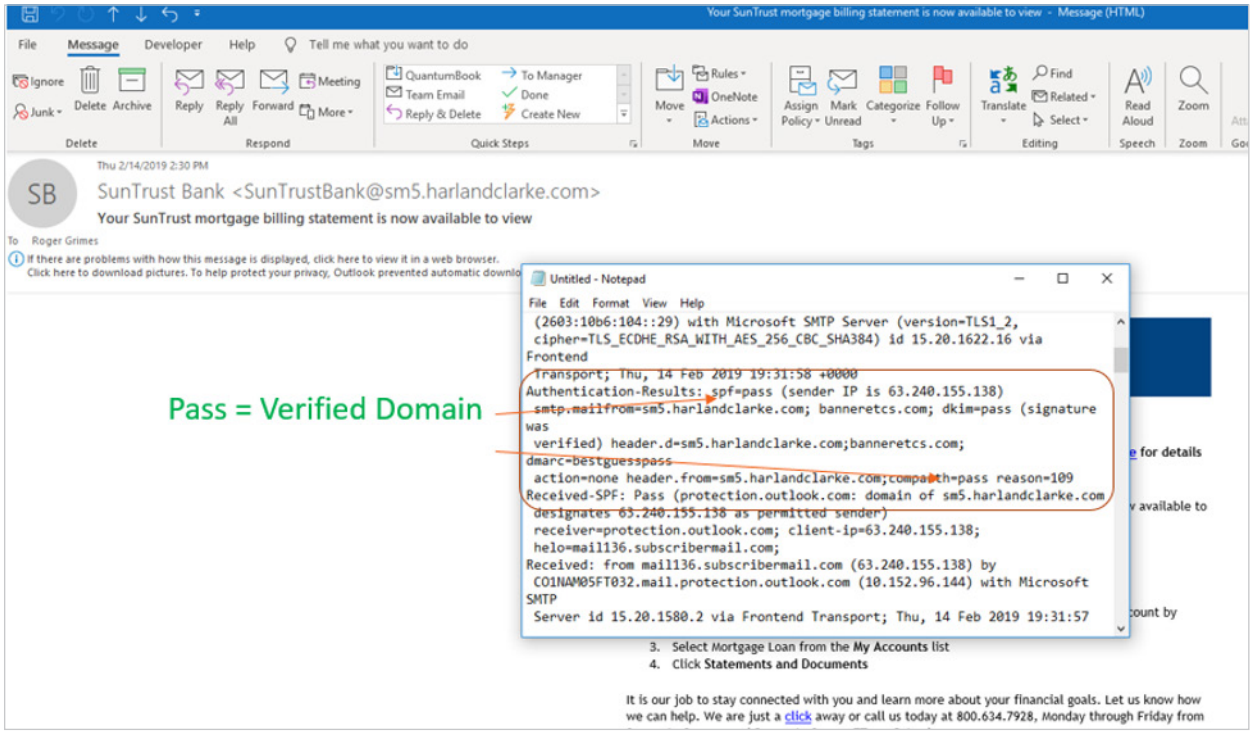
The latter wizard will help you craft the necessary DNS record based on your query answers.

If still in doubt, contact your ISP or email domain provider. They should get this request enough that telling you what you need to include in the DNS TXT record should be easy. Here's some simple SPF example TXT records:

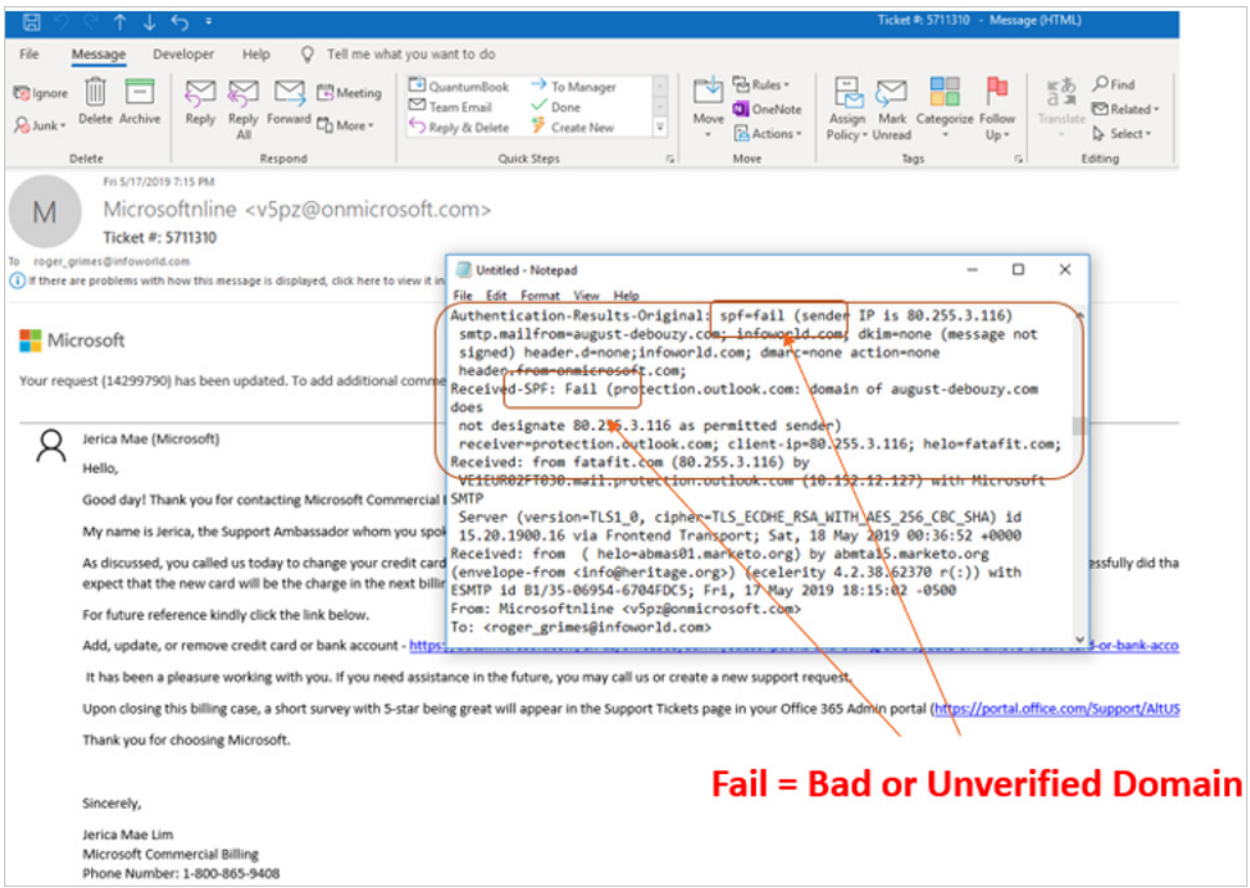
- example.com. IN TXT "v=spf1 -all"
- example.com. IN TXT "v=spf1 a ip4:192.168.1.1 ~all"

Microsoft Office 365 (0365) users should refer to http://knowledge.ondmarc.com/microsoft-office-365/office-365-spf-and-dkim-set-up in order to enable SPF for their domain.

Here's what a verified SPF email header looks like once it gets to an email client:



Here's what a verified "failed" SPF header looks like once it has gotten to an email client:



Remember with all of these technologies, the end user is not usually examining headers or determining whether or not to look at a particular email. This is all done in the background by the receiving email server/service, although understanding what the headers look like in pass and fail modes can help those of us who care enough to examine the headers when we see a suspicious email.

Using DKIM

DKIM is used to prevent the sender's Display Name (5322 address) email address domain spoofing by the receiver verifying the digital signature of the mail server domain sent with each email. DKIM takes a bit more knowledge than SPF to setup. It will require that sender's email server/service itself get at least slightly modified. The sender has to create/get a cryptographic public/private key pair, install it on his/her email server/service, and then create a DNS TXT record which contains his/her public key. Each outgoing sent email is signed by the email server's private key and receivers can verify the digitally signed email by using the sender's public key.

Here are some handy links for setting up DKIM:
https://www.mailjet.com/blog/news/setting-up-dkim-step-by-step-a7d0a0ec-c4aa-4b5b-aeb5-a06361aa2e51/
http://www.gettingemaildelivered.com/dkim-explained-how-to-set-up-and-use-domainkeys-identified-mail-effectively

An example DKIM DNS TXT Record looks similar to:

> *selector._domainkey.example.com IN TXT "v=DKIM1;p=RAG...123"*

"p" is the public key of email server in Base64 format.

Here is an example DKIM email header:

```
DomainKey-Signature: q=dns; a=rsa-sha1; c=nofws;
        s=dkim2014q3; d=sm5.harlandclarke.com;
        h=DKIM-Signature:MIME-Version:Message-ID:X-SM-Email-Key:Content-Type:X-
mid:X-ppid:Subject:Reply-To:To:From:X-appid:List-Unsubscribe:Date:X-dit;
        b=FmR7lFaj+TueNTwhVx5uHkANPkWiTltfr/iJ1nmHI407FxLOriqPsrTCC6Vg2Uxf
        soFpUlpO23VDnzRhhvsB6vbt7TNU1D6vynx3+zRmXOnzw/T3u5dfo00ctwm/0fxq
        ksQqXuGHIn6bZ3V67IRJcbDUrD9FtgaTED/WLaTYNFQ=
DKIM-Signature: v=1; a=rsa-sha1; d=sm5.harlandclarke.com; s=dkim2014q3;
c=relaxed/simple;
        q=dns/txt; i=@sm5.harlandclarke.com; t=1550172717;
        h=From:Subject:Date;
        bh=xcDeDjuUmtqYwVNulH/MIi6s53k=;
        b=XSBvB3TppRpjoEkKt0vCEWqpcDFyNglKjTAlDJpJm9RfpJtD7NjY4zoqczwwxyMW
        H4r+LdAJFNfvufjm+mbbzU8RHo7pM7C32MPRBt8BSKfEi/OOKxR78U5aUBJUlaTf
        2WW0mvZTbsEEvKC3khL6b2or7LXVqYsO3qkfWvxbkok=;
```

Here is an example of a DKIM email header successfully verified:

```
Received: from CO1NAM05FT032.eop-nam05.prod.protection.outlook.com
 (2a01:111:f400:7e50::207) by CO2PR04CA0151.outlook.office365.com
 (2603:10b6:104::29) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384) id 15.20.1622.16 via Frontend
 Transport; Thu, 14 Feb 2019 19:31:58 +0000
Authentication-Results: spf=pass (sender IP is 63.240.155.138)
 smtp.mailfrom=sm5.harlandclarke.com; banneretcs.com; dkim=pass (signature was
 verified) header.d=sm5.harlandclarke.com;banneretcs.com; dmarc=bestguesspass
 action=none header.from=sm5.harlandclarke.com;compauth=pass reason=109
```

Using DMARC

DMARC is simply an aggregator service for whether or not the sender uses SPF and DKIM, and how the sender recommends receivers should treat failed/spoofed emails claiming to be from the sender's domain. Like SPF and DKIM, it is setup in DNS as a TXT record by the sender.

Here are some handy, useful links regarding DMARC:
https://www.validity.com/demystifying-the-dmarc-record/
https://www.validity.com/build-your-dmarc-record-in-15-minutes-2/
http://www.gettingemaildelivered.com/how-to-set-up-dmarc-email-authentication

An example DMARC DNS TXT record might look similar to this:

> *TXT IN "v=DMARC1;p=quarantine;pct=100;rua=mailto:dmarccheck@example.com;"*

One of the most important fields is the p value, which indicates how the sender wants receivers to treat failed emails. P can be one of three values:

- **None** – Take no special treatment for failed emails
- **Quarantine** – Treat as suspicious
- **Reject** – Reject email at server before it gets to client

Be aware that legitimate emails fail one or more SPF, DKIM, and DMARC check routinely. This is often because someone configured something wrong, the email gets incorrectly manipulated in such a way to make it fail one or more of the tests, and over a dozen other reasons. Anyone choosing the REJECT action will probably be killed by management or their end users because they did not get many legitimate emails. So, be safe and go with QUARANTINE instead. Unfortunately, even then, many email services will just act as if NONE was specified.

Not Perfect

SPF, DKIM, DMARC are not perfect for many reasons, including these:

- Hacker could be sending a malicious email from within a compromised domain environment.
- Hacker could be using a domain which enables and uses SPF and DKIM.
- Many commercial email hosts do not respect your settings or all settings. Many times, it's due to the way large email hosts work using many servers over many changing IP addresses to send email on behalf of your domain.

Still, even with the flaws, enabling SPF, DKIM, and DMARC can only help you. When enabled, it will cut down on some portion of your fraudulently received spoof emails. And that is only good.

Just be sure to never completely reject any email which fails one or more verification tests. Legitimate emails fail these checks all the time. You want to set SPF, DKIM, and DMARC so that they will let any failed email be inspected more thoroughly (i.e., quarantined). That way, a human defender can manually inspect the email and decide if it is legitimate or not. If you find that SPF, DKIM, or DMARC causes too many problems, you can always lessen their impact by choosing even less aggressive settings, or if a complete failure, disabling all together (although I've not seen anyone who has had to do this yet).

If an organization hasn't enabled SPF, DKIM, and DMARC, it should. They can only help.

Significant parts of this article first appeared here: https://www.csoonline.com/article/3402016/3-email-security-protocols-that-help-prevent-address-spoofing-how-to-use-them.html

A one-hour KnowBe4 webinar on this topic can be watched here:
https://info.knowbe4.com/dmarc-spf-dkim-webinar

Network Traffic Analysis

Malware and hackers often establish unusual network connections within a compromised network or outbound to the Internet to destinations that the originating network would never connect to during the normal course of business. One of the best methods for detecting hard-to-find malware or hacker exploitation is through network traffic flow analysis.

Here's the basic idea: Most servers don't talk to other servers. Most servers don't connect to most workstations. Workstations almost never talk to another workstation. Most workstations don't talk to every server. Most workstations don't connect to the Internet using server-to-server protocols (e.g., SMTP, POP, IMAP, etc.). Malware and hackers don't appreciate the subtle of what normally connects with what and how. They are usually unaware and uncaring of the legitimate, normal traffic flows, and in any case, don't expect anyone to be looking for unusual connections. Thus, if you understand the legitimate, expected network traffic flows in your environment, you can discover badness with a tool that detects abnormal network flows and generates alerts.

To do this, you need a good netflow analysis tool. Many network packet analysis programs do a decent job at the necessary data collection and netflow representation, but are not dedicated to netflow analysis. There are open source and commercial tools dedicated to netflow analysis, which can be found by simply searching on 'netflow analysis'.

Data-Leak Monitoring and Prevention

Data-Leak monitoring and prevention tools can prevent critical data from leaving the safe confines of an organization's network. Any tool which you can use to prevent data leaks, however they occur, should be considered as part of your defense.

Honeypots/Deception Technology

A honeypot is a computer device or resource which exists solely to detect hackers and malware. Many vendors offer "deception technology" devices and software which can mimic many different devices, operating systems, and servers. You can also take a production device or server you are getting ready to decommission because it is becoming aged or no longer needed and turn it into a honeypot. Since it's not a production asset, no one should be trying to log into it. If someone tries to login to a honeypot, it almost always indicates unauthorized activity and potential maliciousness. Honeypots are low cost, high value, early warning assets that should be a part of anyone's environment.

Extreme Control: Red/Green Systems

In some environments with low risk tolerances and extremely high value of assets which can easily be stolen, senior management has decided to provide all users with two systems: colloquially known in academic circles as red/green systems. The red system is highly secured and only contains mission-critical business software and services. Users can only do business tasks on their red system. The green system is a less secured system and can be used by the employee to do Internet surfing, personal tasks, and email. The idea is to take the highest risk tasks (such as surfing the web and picking up email) and physically separate them from the mission-critical assets and data.

Early on, organizations implementing red/green systems used two physical computers. Today, it is more likely to be accomplished logically using two different virtual machines. Today, some organizations even used highly locked down virtual computers or desktops, which still appear to the end user as a single desktop to him/her. But the different icons and applications they click on belong to and execute in highly separated, secured areas, so that the exploitation of one side (in the green side usually) does not impact the other side (usually the red side).

Red/Green system implementations do significantly reduce risk, but it doesn't eliminate all risks. There are always tasks that will cross over between red and green systems that the user is involved in, and if this is the case, social engineering of the human is still possible. Still, it does significantly reduce many risks. The downside is that providing two different physical systems to one person nearly doubles operational costs. It's two pieces of hardware to buy, provide, and support. It's two network connections. It is additional licenses. Using virtual machines significantly reduces those costs and licenses, but still results in higher operational costs. But for some organizations, it is the right solution for their level of risk and asset value.

Technical Defenses Summary

Every organization needs to decide which technical defenses they can afford, deploy, and support to fight cybersecurity threats. A complete, defense-in-depth defense requires far more than was covered in this document, but this section did cover the most common technical defenses involved directly with fighting social engineering and phishing.

TRAINING BEST PRACTICES TO FIGHT SOCIAL ENGINEERING AND PHISHING

This section summarizes the security awareness best practices that any organization should have to effectively fight social engineering and phishing.

Overall Goal

You overall goal should be to change your organization's overall culture so that all employees actively work to reduce risk from cybersecurity threats, and for this document, particularly threats from social engineering and phishing. No matter how well thought out and deployed, some amount of social engineering and phishing will always get past your policies and technical defenses, so training is needed to help users recognize threats and to take the appropriate actions.

Security Awareness Training Cycle

KnowBe4 has been providing elite security awareness training services, tools, and methodologies since 2010. Customers following our recommendations significantly reduce the risk of hacker or malware success due to social engineering and malware. As shown in the graphic below, KnowBe4 customers have an average risk reduction of 87% in one year. They take the "Phish-Prone™" percentage of employees from almost 38% to less than 5% in a year. It would be difficult to find another computer security defense with a better, demonstrated risk reduction.

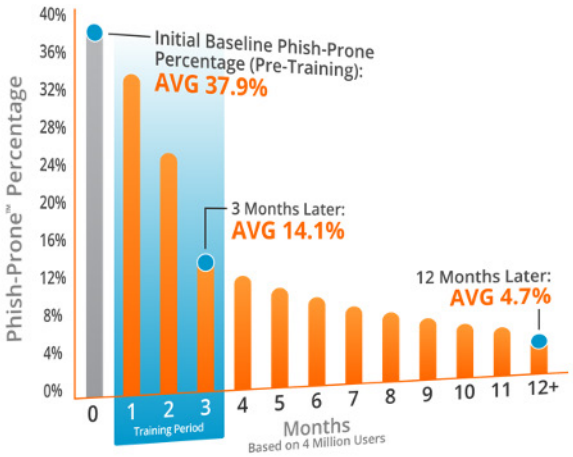
Generating Industry-Leading Results and ROI

- Reduced Malware Infections
- Reduced Data Loss
- Reduced Potential Cyber-theft
- Increased User Productivity
- Users Have Security Top of Mind

87% Average Improvement

Across all industries and sizes from baseline testing to one year or more of ongoing training and testing

Note: The initial Phish-Prone percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 platform prior to the evaluation. Subsequent time periods reflect Phish-Prone percentages for the subset of users who received training with the KnowBe4 platform.



Source: 2020 KnowBe4 Phishing by Industry Benchmarking Report

KnowBe4's security awareness training recommendation is a four-step cycle (as represented graphically below). This security awareness training cycle is recommended no matter what tools you use, but of course, we believe KnowBe4 has the best combination of tools and content to help any organization to be as successful as possible.

KnowBe4 Security Awareness Training

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

Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users
Best-in-class, fully automated simulated phishing attacks, thousands 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!

Baseline Testing

Every organization needs to start their anti-phishing security awareness training program with baseline testing. You want to establish a baseline of which employees and percentages of employees who are most susceptible to phishing by sending out a simulated phishing campaign and measuring who opens or responds to the simulated phishing attempt. Most organizations that do this find upwards of 38% of their employees are easily tricked into responding to (i.e., providing login credentials, opening potentially malicious file attachments, etc.) to phishing attempts. This is not good and points to why hackers so frequently rely on and use social engineering and phishing.

It's also important to do an initial baseline so that you can show the success of your security awareness training program using easy-to-see and verify data. Sadly, so much of the computer security world is full of false promises and made-up statistics. Comparing how many of your employees are susceptible to phishing at the beginning of your security awareness training program versus at a later date will allow you to measure its overall success and allow you to focus on people who require more focus.

Train

Provide/require training on at least a monthly basis, if not more frequently. Our data has shown that training only annually provides almost no benefit. No measurable benefit begins to be noticed until training occurs at least quarterly. But the sweet spot is training provided at least monthly, if not more. Longer training should be provided when an employee is hired, and annually thereafter. And then shorter trainings provided each month.

Training should include popular phishing and social engineering topics, and be updated as phishing and social engineering trends emerge. Phishers and social engineers love to use topical (e.g. COVID-19, natural disasters, and popular culture) events to get more potential victims to open up their phishes and run their Trojan Horse programs. Training should always include the perennial core anti-social engineering and anti-phishing topics that are always tried, such as requests for login credentials and requests to install fake critical security patches.

Training should use a variety of methods, including videos, posters, quizzes, and games. KnowBe4 has more content and more variety of training content than any other competitor. We have over 1,000 pieces of separate content, over a variety of different tones and methods, available in over 30 languages. Our content is made by a large team of global computer security experts and professional educators. Our content isn't just made by one or two people who are good at computer security videos. Many of our content offerings include quizzes to gauge how well the trainee understood the content.

Simulated Phishing Campaigns

Every organization should routinely conduct simulated phishing campaigns against all stakeholders. Simulated phishing campaigns should start with simple, somewhat easy-to-spot, low-sophistication phishing tests. As your employees improve their ability to spot these easy phishing tests, the simulated phishing campaigns should get more sophisticated and more difficult to easily spot as a phishing email. As your organization's culture of security awareness increases, the 'level of difficulty' of the involved phishing tests should increase over time.

Years ago, many organizations wondered if testing employees with "fake" phishing emails was necessary or even ethical. Today, most organizations understand the value and do not question its validity. Testing someone with a simulated phishing email is an essential part of someone's training. It not only tests how well someone understands and implements anti-phishing education, but is part of the educational process.

It reinforces previously taught information and turns looking for signs of social engineering and phishing into a game. Every organization administrator who has deployed simulated phishing campaigns can tell you the stories of employees thinking they were reporting a simulated phishing email only to be told that the email they reported was a real-world phish instead. Simulated phishing skills builds knowledge, expertise, and confidence.

KnowBe4 recommends that all organizations conduct monthly or more frequent simulated phishing campaigns. These phishing campaigns should simulate common real-world phishing attacks. They should send out simulated phishing campaigns at random intervals instead of to all employees all

at the same time. You don't want a single knowledgeable employee spotting a simulated phishing attack and warning everyone else. You want to mix up topics, using simulations which mimic types of real-world spear phishing attacks, along with general, common phishing methods.

Simulated phishing campaigns should include a mix of credential requests and requests for people to open potentially malicious file attachments. The organizations with the most mature security awareness training programs should attempt to do simulated phishing campaigns using methods above and beyond email (e.g., voice calls, SMS, etc.).

There is no question that organizations doing routine simulated phishing campaigns reduce cybersecurity risk faster and better. Don't let real hackers and scammers be the only people who are testing your employees.

Analyze

Hopefully the security awareness training you are using is providing reliable, actionable data, like KnowBe4's systems do. At the bare minimum, you want to be able to identify stakeholders who are failing an above average number of simulated phishing campaign tests, so that they can be given additional training, as needed. You can identify individuals who need more training and identify departments and locations who seem to need more training in aggregate. In KnowBe4's systems, how every individual did on every simulated phishing campaign and how they interacted with the phishing emails are reported, along with any taken and outstanding training courses. The individual's role, training, and results from the simulated phishing testing campaigns end up creating an individual risk score which can be tracked over time. Every individual's risk score can be aggregated into a group/department risk score. Group scores can be aggregated up into an overall organizational risk score (example shown below). Administrators and senior management can see the organization's risk score improvement (hopefully) over time.

No matter how you do it, organizations doing security awareness training should get and use good data to allow them to modify training as needed and to show the change in cybersecurity risk over time. There is no better way to show the value of security awareness training than to show the supporting data.

Professional Hints

This section contains some more advanced topics for helping to improve security awareness training.

Make Them Care

It is difficult to change any individual's behavior, much less change an entire organization's computer security culture. Still, it can help anyone charged with the responsibility of their organization's security awareness training to understand how to change individual behavior as part of changing their organization's culture. KnowBe4's Perry Carpenter's book Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors is a great resource to read in this regard.

One of the book's core tenets is: "They [employees] may be aware and still not care."

Here's how you make them care. There are two keys: First, imparting the importance and second, incentives.

Communicate the Importance of Security Awareness Training

Part of the problem is that most users have no idea how big of a role security awareness training can play in their fight against social engineering and phishing as compared to other defenses. Users are told they have to do a "hundred different things" to fight computer crime, such as "Make sure your software is patched", "Make sure to lock your desktop when you are away", "Don't click on unexpected file attachments", and "Make sure your password is long and complex". Users hear so many rules and recommendations that they can't figure out which one is or isn't as important as another. There is very little teaching of relevance in the computer security world. It's as if we treated playing with Nerf darts the same as playing with real guns. Both can cause injury, but one is more likely to result in serious, long-lasting injury than another.

But if you share the facts (as shared at the beginning of this document), that nothing could be as important to the cybersecurity of an organization as fighting social engineering (and show them using data and pictures), it helps to provide relevance and focus. To reiterate the main points, according to nearly every study done on computer security crime for over a decade, social engineering and phishing are responsible for more cybersecurity incidents than any other cause. Social engineering and phishing are responsible for 70% to 90% (https://blog.knowbe4.com/70-to-90-of-all-malicious-breaches-are-due-to-social-engineering-and-phishing-attacks) of security breaches. Unpatched software is responsible for 20% to 40% of malicious data breaches. Nothing else comes close. All other types of computer crime (e.g., password attacks, eavesdropping, misconfiguration, insider attacks, etc.) amount to just 1% to 10% of malicious data breaches.

This means there is nothing else that matters as much to reduce cybersecurity risk as focusing on defeating social engineering and phishing. This also means that if an organization doesn't effectively mitigate social engineering and phishing, nothing else matters.

Incentives

Incentivizing people to want to take training doesn't hurt, especially if they first understand and care why they have to take it. Incentives can include positive feedback, social recognition, small gifts, gift cards, money, and bonuses.

Offer Interesting Training

Most employees have had enough boring, staid training. So, give them more exciting education. For example, at KnowBe4, our award-winning, Netflix-like, The Inside Man series is loved by almost every person who takes it. It's not going to win an Oscar, although it did win a Silver Telly Award, which honors video and television made for all screens. It's pretty great. The Inside Man uses professional actors with professional production values and a mystery-driven narrative to show and teach computer security defenses. No one can believe that it is training. We have security administrators and employees asking when the next episodes will be out. When does that ever happen with training? Well, it does with The Inside Man.

Switch It Up

Make sure you switch up training content. Try different things. Different people learn differently. At KnowBe4, our extensive content spans across just about every type of learning style you can imagine—videos, documents, posters, quizzes, and even cartoons. Even if someone loves a particular style of learning, say The Inside Man, it can't hurt to switch it up every now and then. Maybe switch to a cartoon or send around a security training poster, like KnowBe4's Social Engineering Red Flags PDF shown above.

Don't Underestimate the Power of a Certificate

It's amazing what a printed certificate of achievement can do to brighten someone's outlook. Many organizations recognize employees who go a quarter or year without failing a simulated phishing test with a certificate suitable for hanging. It's a small, nearly cost-free action that will result in a tremendous amount of goodwill and feeling of accomplishment in many employees. It's not the paper they love, it's the recognition of their accomplishments by an organization that shows it cares.

Offer Free Training for Families

Nothing makes people care more than if you care about them and their families. All KnowBe4 customers get content that is meant to be shared with their families. When mom or dad is sharing tips on how not to be socially engineered or phished with their children, the more likely they are to be better trained for work.

Teach Like a Marketer

The best ad campaigns are frequent, redundant, and entertaining. This is not accidental. Over a hundred years of ad campaigns have taught marketers that these attributes are the best way to get potential customers to remember and buy a product. So, train like a marketer. Training needs to be frequent. How frequent? At least once a quarter. Anything less than that has no impact on decreasing risk. The best cost/benefit is found with training at least once a month, and more frequent is better.

Most people are very busy and don't remember every detail they are told about everything the first time they are told. It normally takes at least three repeats of the same material for people to start to remember something. More often reinforces the educational information. Many organizations are afraid to repeat the same information over and over for fear of boring the user. But if you think about the most critical safety behaviors you had to learn, such as looking both ways before crossing a road, driving a car, and how not to run holding a knife, those lessons were repeated over and over to you until they became second nature. Now, you likely look unconsciously both ways before crossing a street without even thinking about it. You want your repeated security awareness training messages to be frequent and redundant. This doesn't mean the same message has to be delivered in the same way. You can switch it up and vary the channel used.

The best training is informative AND entertaining. The more entertaining it is, the more likely it is that your employees will pay attention to it. Think about the television commercials you remember and love the most—they are entertaining. You want to do the same thing with your security awareness training. As previously mentioned before, KnowBe4's The Inside Man series has been described by many fans as the most enjoyable security awareness training they have ever experienced.

Keep up to Date With Latest Phishing Trends

It is key that security awareness training advocates keep up with the latest phishing trends. What was popular two years ago is often not popular today. For example, until a few years ago, fake antivirus software phishing emails were a common method for social engineering Trojan Horse programs onto victims' computers. Today, fake antivirus scams are usually accomplished over phones from organizations pretending to be proactively notifying the victims of a virus infection. When the phishing scams change, so too, does the education. KnowBe4 helps people keep up with the most popular scams at the moment using a variety of education tools, including the methods below.

Common In the Wild Attacks

Put out once a quarter, the KnowBe4 Common in the Wild Attacks is a global threat intelligence data point listing either popular or interesting real-life phishing emails reported by PAB users, followed by the key takeaway to communicate to your users for those attacks.

Example Top 10 Common in the Wild Attacks

Reported Phishes of the Week

Reported Phishes of the Week (see example below) are included in a list of the most popular or interesting reported phishing emails (by KnowBe4 phishing template) reported by PAB users each week. Many KnowBe4 admins automate sending these simulated phishing emails to all end users using a randomized time and date. With ten brand new templates each week, using this category of KnowBe4 templates will allow you test your users with a variety of real-life phishing attacks.

Example Reported Phishes of the Week

REPORTED PHISHES OF THE WEEK

"Account report": Phish prompts reader to open attachment to view information on cash account problems.

"Alert: Your [[domain]] Email is at Risk!": Fake GoDaddy email asks users to log in to upgrade account.

"Booking confirmation": Phish prompts readers to open attachment to view booking/confirmation information.

"Booking information -- Conf. No. 87415": Fake Lufthansa email baits readers to click link to check flight information.

"Budget Report": Phish invites readers to view budget report by clicking link.

"Confirmation letter": Phish asks users to click on link to review load confirmation letter.

"Invoice 80521": Fake medical center invoice baits users to click link to view more information.

"Status Alert": Fake Amazon email prompts user to log in to update account information.

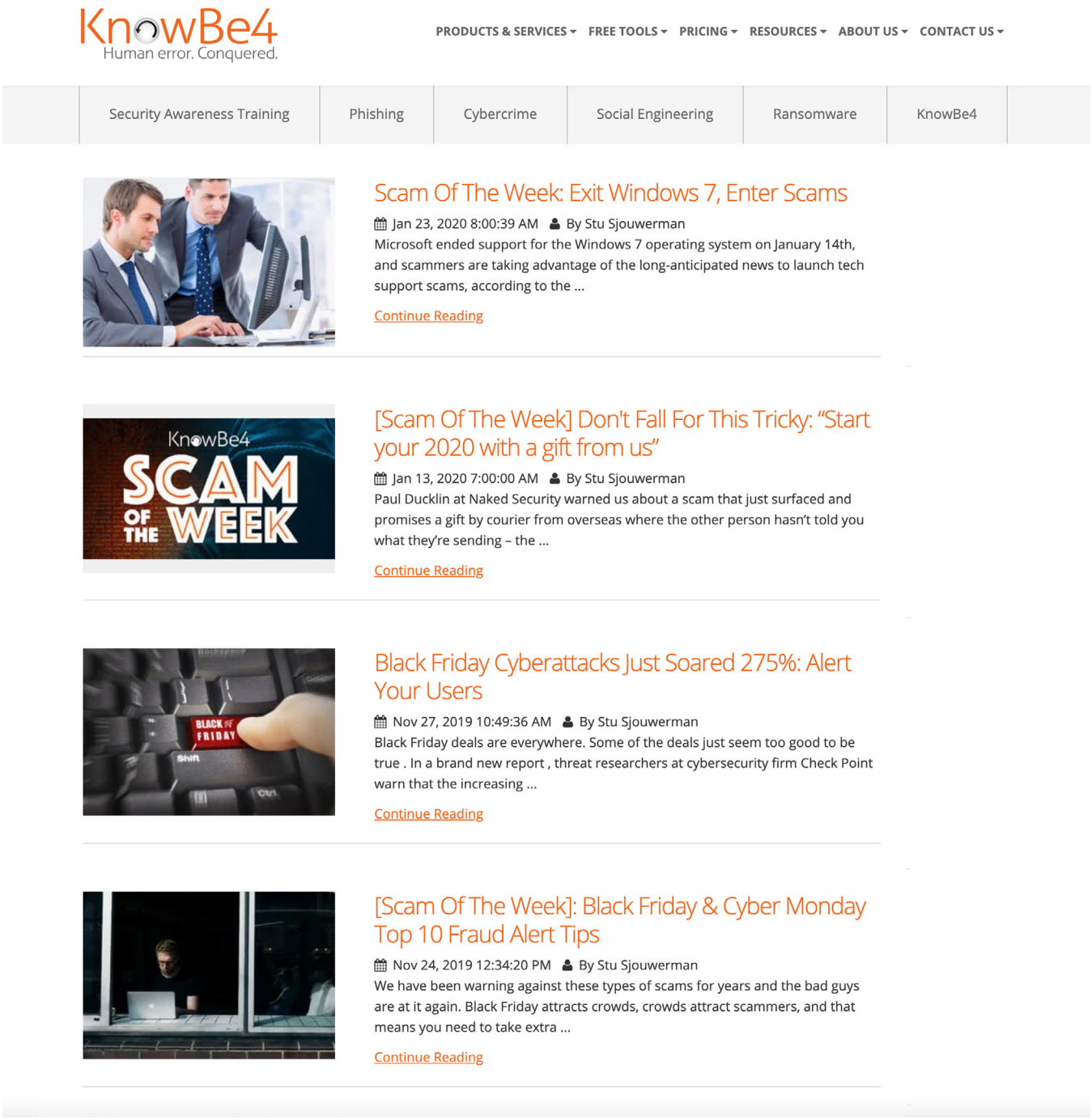
"TT COPY": Malicious email attachment purports to contain information on wire transfer.

"Your account was restricted - Urgent": Fake LinkedIn email requests users to verify account by clicking link.

Learn more about Reported Phishes of the Week here:
https://blog.knowbe4.com/reported-phishes-of-the-week
https://support.knowbe4.com/hc/en-us/articles/227803307-What-is-the-Reported-Phishes-of-the-Week-Category-

Scams of the Week

Scams of the Week (see example below) are selected phishing and social engineering examples as determined by Stu Sjouwerman, CEO of KnowBe4. Stu has been involved in security awareness training for a very long time, and he has a talent for spotting the interesting cases and the ones likely to become more prevalent over time. As is the case with most of these global threat intelligence feeds, Scam of the Week is a KnowBe4 template type that can be used in simulated phishing campaigns, or it can be used as a powerful training resource for end users.

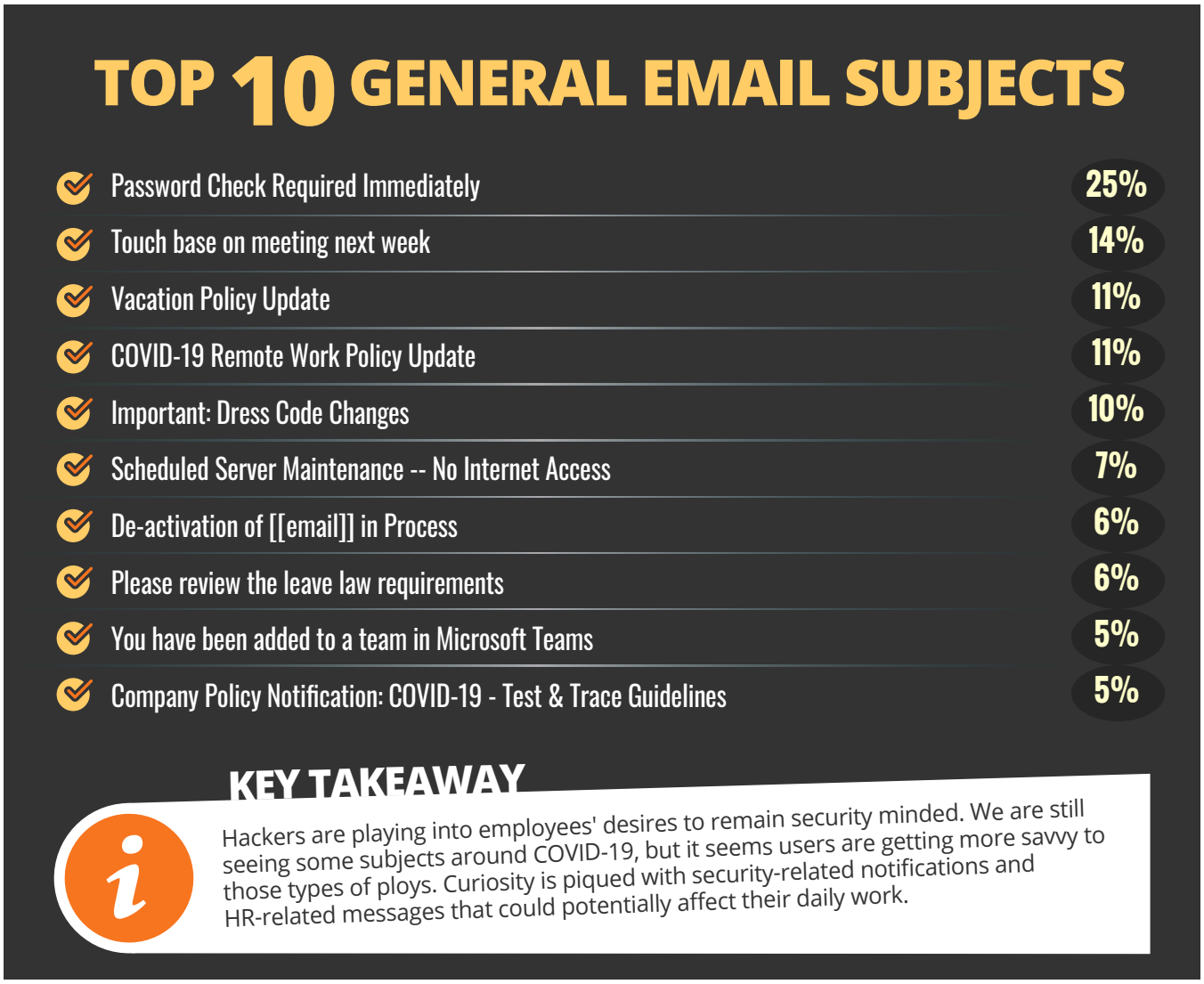


To learn more about Scams of the Week, visit:
https://blog.knowbe4.com/topic/scam-of-the-week
https://support.knowbe4.com/hc/en-us/articles/226314167-How-to-Set-Up-a-Scam-of-the-Week-Newsletter

Top-Clicked Phishing Tests

Published quarterly, the Top 10 General Email Subjects global threat intelligence feed lists the top simulated phishing email subjects as reported by PAB users, along with a key training takeaway (see example below).

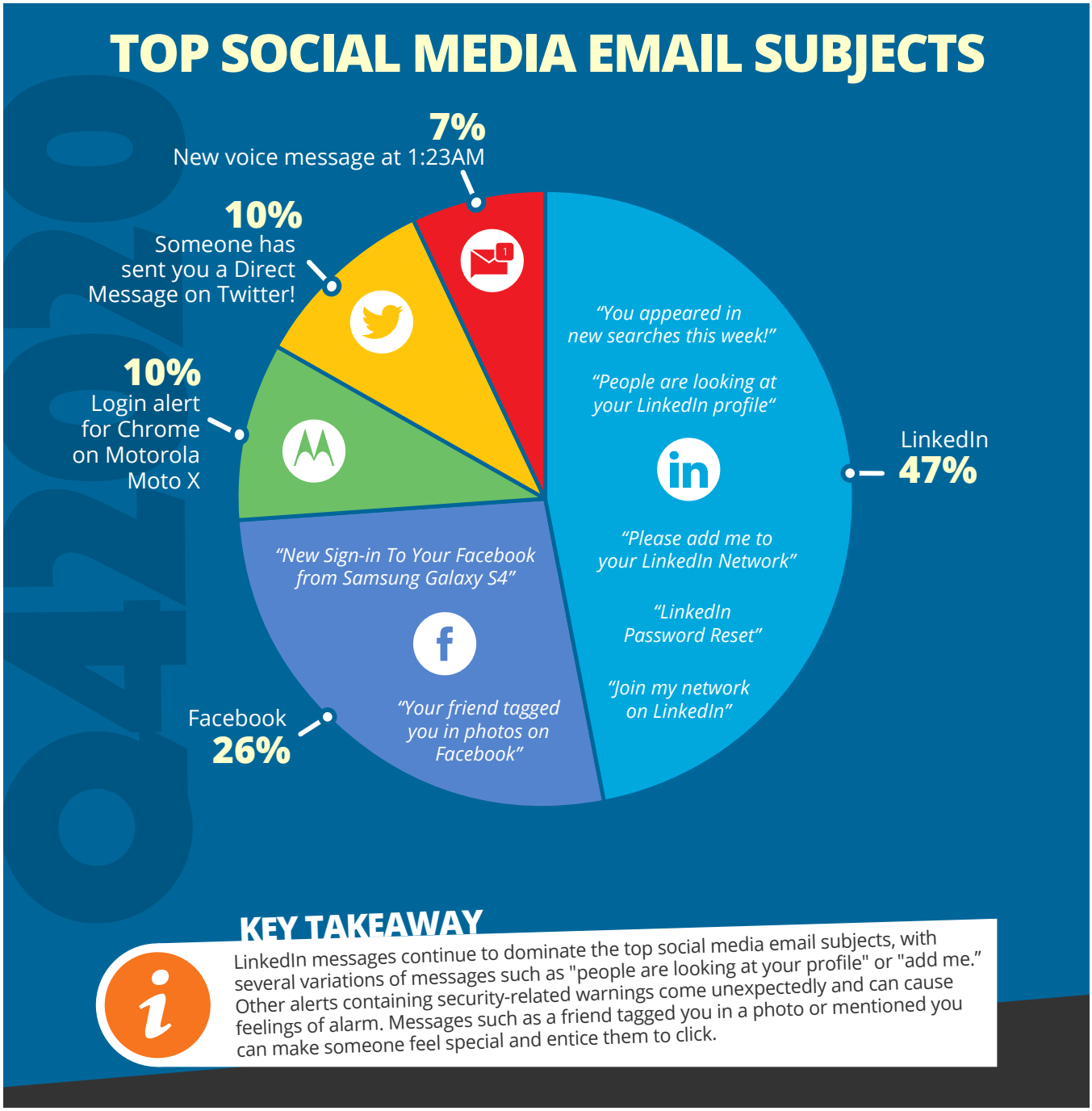
Example Top 10 Clicked Phishing Tests



Top Social Media Phishing Tests

Many corporate data breaches began as social media phishes. Even if you're starting to get a handle on phishing at work, social media is a top way your employees are successfully phished at home. KnowBe4's quarterly released Top Social Media Email Subjects (see example below) lists the most popular or interesting social media email subjects as reported by PAB users.

Example Top Social Media Email Subjects



Many of these documents are available as templates which can be inserted into a simulated phishing or training plan.

Security Advocates/Champions/Heroes

The best computer security educator can only be spread so thin. We are big fans of organizations using local security awareness training experts and their stories and local experience to help drive that education home. When end users see local people caring and evangelizing security awareness training, it helps the lessons to sink in more than for someone who is "forced" to watch a training video once a year. But we also realize that most organizations don't have the time or resources to have one person or team develop those one-on-one relationships, especially in larger organizations. That's where having a team of volunteer proactive security awareness advocates can help.

Many organizations create special programs to leverage good content and local people to spread the message and improve the culture. The programs have different names (i.e., Advocates, Champions, Security Guardians, Sentinels, etc.) but they all invite volunteers to help educate everyone else in some small way. They will benefit organizations of any size.

Test Out Quizzes

Use a "test-out" quiz as a way to get people who are normally resistant to training to proactively take the training. They think they are taking a quiz to avoid the training, but in actuality, they are taking the intended training.

If you're a KnowBe4 customer, you can select amongst many pre-built quizzes, and even have people automatically registered for longer training if they "fail". You can even upload your own custom quiz. If you do, create each question with enough scenario detail and training to cover what you otherwise would have during the actual, longer training. Make a lot of the answers be "All of the Above" and have all those answers be the training content. If designed correctly, the quiz will be fairly easy to pass. It's meant to be. You're more concerned about exposing people to the content and having them learn as part of the process than a real pass/fail test of knowledge.

Example of "Test Out" Easy Quiz Question:

Which of the following statements are true?

A Social engineering and phishing account for the majority of all malicious data breaches.

B Unpatched software is the second most commonly used hacker attack method.

C User passwords should not be easy to guess and should be unique for every network and/or website.

D All of the above are true.

Turns out using a test out quiz is a great way to pass along the education you were hoping to share with people who would otherwise not be inclined to watch a video or read a document.

Culture

Security isn't just IT's problem, but everyone's problem within the organization. The key isn't "yet another security solution", but a changing of the way the organization thinks about cybersecurity. The key to stopping cyber attacks from being successful revolves around every part of the organization being concerned about security. IT is already on top of this, but you need the C-Suite, HR, and users all on board—each one working towards a more secure way of operating.

The success of security firmly rests in whether a culture exists that perpetuates both the need for security and the use of security in everyday work. This cultural shift requires a paradigm change where nearly every part of the organization plays a role:

- **Senior leadership** – You are perfectly situated with visibility into the entire organization, able to see the results of a change in culture. You also have the ability to mandate an organization-wide collaboration towards building a security culture.
- **HR leadership** – You understand the pulse of the organization. As the culture shifts towards including security as a daily aspect of the job, you can ensure employees understand why it's important, obtaining valuable feedback from users on how the culture change impacts them, then providing this to IT.
- **IT leadership** – You are the bridge between the business, operational, security, and technology requirements necessary to create and maintain this culture change.
- **Security staff** – You can help assess risk, develop strategy, ensuring reporting and accountability around implemented technologies and processes that drive culture change.
- **IT staff** – You can help to identify and implement solutions that will augment the security culture. A focus on simplified adoption and ease of use, matched with an actual ability to make the organization safer is something required of someone close to both the organization's technology and users.
- **Users** – You can incorporate security awareness into your daily work activities, being cognizant of the need to be on alert when interacting with anything outside the organization (e.g., email, websites, phone calls, etc.), as well as the need for good security hygiene around passwords and data security.

Creating a security culture takes a village—and, in this case, the village is under constant attack. It's time to do more than just sharpen spears and post lookout points; it's time to employ the entire village to participate in ensuring security.

Training Summary

Some amount of phishing and social engineering will always bypass the best policy and technical defenses. Considering that it is very important to train employees in how to recognize when that happens and how to treat it. Social engineering and phishing have long been the number one cause for malicious data breaches. Use good security awareness training to build a human firewall.

CHECKLIST SUMMARY

This section summarizes the policies, technical defenses, and training best practices that any organization can have to effectively fight social engineering and phishing in an easy-to-quickly-review checklist format.

Checklist Item	Checkmark
Policies	
Acceptable Use Policy which stakeholders sign when hired and at least annually thereafter	✓
Specific Anti-Phishing Policies	
Specific policies to prevent business email compromise scams	
Training Content	
Teach stakeholders how to recognize rogue URLs	
Teach stakeholders how to spot phishing emails using Red Flags of Social Engineering	
Defined and communicated of how someone should handle/treat a simulated phishing test and/or real phishing event	
Defined methods of positive reinforcement for successfully spotting a simulated phishing test and/or real phishing event	
Defined and communicated consequences for failing simulated phishing tests	
Notice of simulated phishing training and methods	
Defined and practiced incident response plan and policies	
Defined and communicated crisis response plan (e.g. when to involve sr mgmt., HR, lawyers, recovery specialists, PR, etc.)	
Defined and practiced disaster recovery/business continuity plan(s)	
Ransomware handling and decision on whether to ever pay ransom	
Cybersecurity Insurance	
Other/Misc.	
Technical Defenses	
Defense-in-Depth plan	
Network security boundary defenses	
Content filtering defenses	
Anti-Phishing identification services/products	

Checklist Item	Checkmark
Feature like Phish Alert Button so stakeholders can easily report attempted phishing attacks	
Detonation sandboxes	
Reputation services	
DNS checks	
Anti-Malware defenses	
Implementing least-permissive permissions	
Email client protections	
Browser protections	
Implementing global phishing standards (SPF, DKIM, and DMARC)	
Network traffic analysis	
Data-leak detection and prevention solutions	
Honeypots/Deception Technologies	
Red/Green Systems?	
Other/Misc.	
Other/Misc.	
Training Best Practices	
Initial simulated phishing baseline test	
Longer, annual training	
Shorter, monthly or more often training	
Monthly or more often simulated phish testing	
Analyze results to determine where to concentrate more	
Professional Hints	
Make them care	
Train like a marketer (e.g. frequent, repeatable, entertaining)	
Offer interesting training	
Use a variety of training methods (e.g. videos, quizzes, documents, games, etc.)	
Create incentives	

Checklist Item	Checkmark
Offer free training for families	
Keep up with the latest phishing trends	
Create security advocates/champions/heroes	
Test out quizzes	
Change your culture	
Other/Misc.	
Other/Misc.	

Check KnowBe4's main website at https://www.knowbe4.com/resources for the latest news and comprehensive set of resources dedicated to helping every organization and person more effectively fight social engineering.

CONCLUSION

There is nothing any organization or individual can do to significantly decrease cybersecurity risk faster and better than to fight social engineering and phishing. This ebook summarized the policies, technical defenses, security awareness training best practices, and selected ideas to consider, that all organizations can deploy to defeat social engineering and phishing.

RESOURCE SUMMARY

Here is a consolidated list of KnowBe4 and other related resources mentioned in this document.

KnowBe4's resources website (https://www.knowbe4.com/resources)

Learning How to Forensically Examine Phishing Emails to Better Protect Your Organization webinar (https://info.knowbe4.com/phishing-forensics)

70% to 90% of all Malicious Breaches Are Due to Social Engineering KnowBe4 blog article (https://blog.knowbe4.com/70-to-90-of-all-malicious-breaches-are-due-to-social-engineering-and-phishing-attacks)

Using Threat Intelligence to Build Your Data-Driven Defense (https://info.knowbe4.com/threat-intelligence-to-build-your-data-driven-defense)

KnowBe4 Glossary of Terms (https://www.knowbe4.com/knowbe4-glossary/)

KnowBe4 Social Engineering Red Flags PDF document (https://www.knowbe4.com/hubfs/Social-Engineering-Red-Flags.pdf)

Share the Red Flags of Social Engineering Infographic With Your Employees blog article (https://blog.knowbe4.com/share-the-red-flags-of-social-engineering-infographic-with-your-employees)

Combatting Rogue URL Tricks: How You Can Quickly Identify and Investigate the Latest Phishing Attacks webinar (https://info.knowbe4.com/rogue-urls)

Top 12 Most Common Rogue URL Tricks blog article (https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks)

Phish Alert Button free tool (https://www.knowbe4.com/free-phish-alert)

PhishER KnowBe4 product (https://www.knowbe4.com/products/phisher)

The FBI Updates Their Numbers And BEC Is Now A 26 Billion Dollar Scam blog article (https://blog.knowbe4.com/the-fbi-updates-their-numbers-and-bec-is-now-a-26-billion-dollar-scam)

CEO Fraud Prevention Manual (https://info.knowbe4.com/ceo-fraud-prevention-manual)

12 Ways to Hack MFA webinar (https://info.knowbe4.com/webinar-12-ways-to-defeat-mfa)

Hacking MFA ebook: (https://info.knowbe4.com/12-way-to-hack-two-factor-authentication)

Multifactor Authentication Security Assessment tool (https://www.knowbe4.com/multi-factor-authentication-security-assessment)

KnowBe4's Multifactor Authentication web portal (https://www.knowbe4.com/how-to-hack-multi-factor-authentication)

Hacking Multifactor Authentication book (https://www.amazon.com/Hacking-Multifactor-Authentication-Roger-Grimes/dp/1119650798)

Cyberheist News, Volume 10, [Eye Opener] Almost Half of Ransomware Attacks Now Involve Data Exfiltration and Extortion (https://blog.knowbe4.com/cyberheistnews-vol-10-46-eye-opener-almost-half-of-ransomware-attacks-now-involve-data-exfiltration-and-extortion)

Now That Ransomware Has Gone Nuclear, How You Can Avoid Becoming the Next Victim KnowBe4 webinar (https://info.knowbe4.com/nuclear-ransomware)

Ransomware Hostage Rescue Manual (https://info.knowbe4.com/ransomware-hostage-rescue-manual-0)

KnowBe4 Ransomware information webportal (https://www.knowbe4.com/ransomware)

KnowBe4's KCM GRC Platform (http://kcmgrc.knowbe4.com/)

Blacklist Master (https://www.blacklistmaster.com/blacklists)

Google's Virustotal (https://virustotal.com)

Useful SPF configuration links include:
https://support.rackspace.com/how-to/create-an-spf-txt-record/
https://www.validity.com/how-to-build-your-spf-record-in-5-simple-steps/
https://stopemailfraud.proofpoint.com/spf/
https://www.spfwizard.com/

Links for setting up DKIM:
https://www.mailjet.com/blog/news/setting-up-dkim-step-by-step-a7d0a0ec-c4aa-4b5b-aeb5-a06361aa2e51/
http://www.gettingemaildelivered.com/dkim-explained-how-to-set-up-and-use-domainkeys-identified-mail-effectively

Links regarding DMARC:
https://www.validity.com/demystifying-the-dmarc-record/
https://www.validity.com/build-your-dmarc-record-in-15-minutes-2/
http://www.gettingemaildelivered.com/how-to-set-up-dmarc-email-authentication

How to Prevent 81% of Phishing Attacks From Sailing Right Into Your Inbox With DMARC webinar (https://info.knowbe4.com/dmarc-spf-dkim-webinar)

KnowBe4 Security Awareness Training (https://www.knowbe4.com/products/enterprise-security-awareness-training)

KnowBe4's Perry Carpenter's book Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors

KnowBe4's award-winning, Netflix-like, The Inside Man series (https://www.knowbe4.com/inside-man)

KnowBe4's Reported Phishes of the Week (https://blog.knowbe4.com/reported-phishes-of-the-week) or (https://support.knowbe4.com/hc/en-us/articles/227803307-What-is-the-Reported-Phishes-of-the-Week-Category-)

KnowBe4's Scams of the Week (https://blog.knowbe4.com/topic/scam-of-the-week) and (https://support.knowbe4.com/hc/en-us/articles/226314167-How-to-Set-Up-a-Scam-of-the-Week-Newsletter)

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4 is the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

V012921