What Is Phishing?

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

Phishing is one of the easiest forms of cyberattack for criminals to carry out, and one of the easiest to fall for. It's also one that can provide everything hackers need to ransack their targets' personal and work accounts.

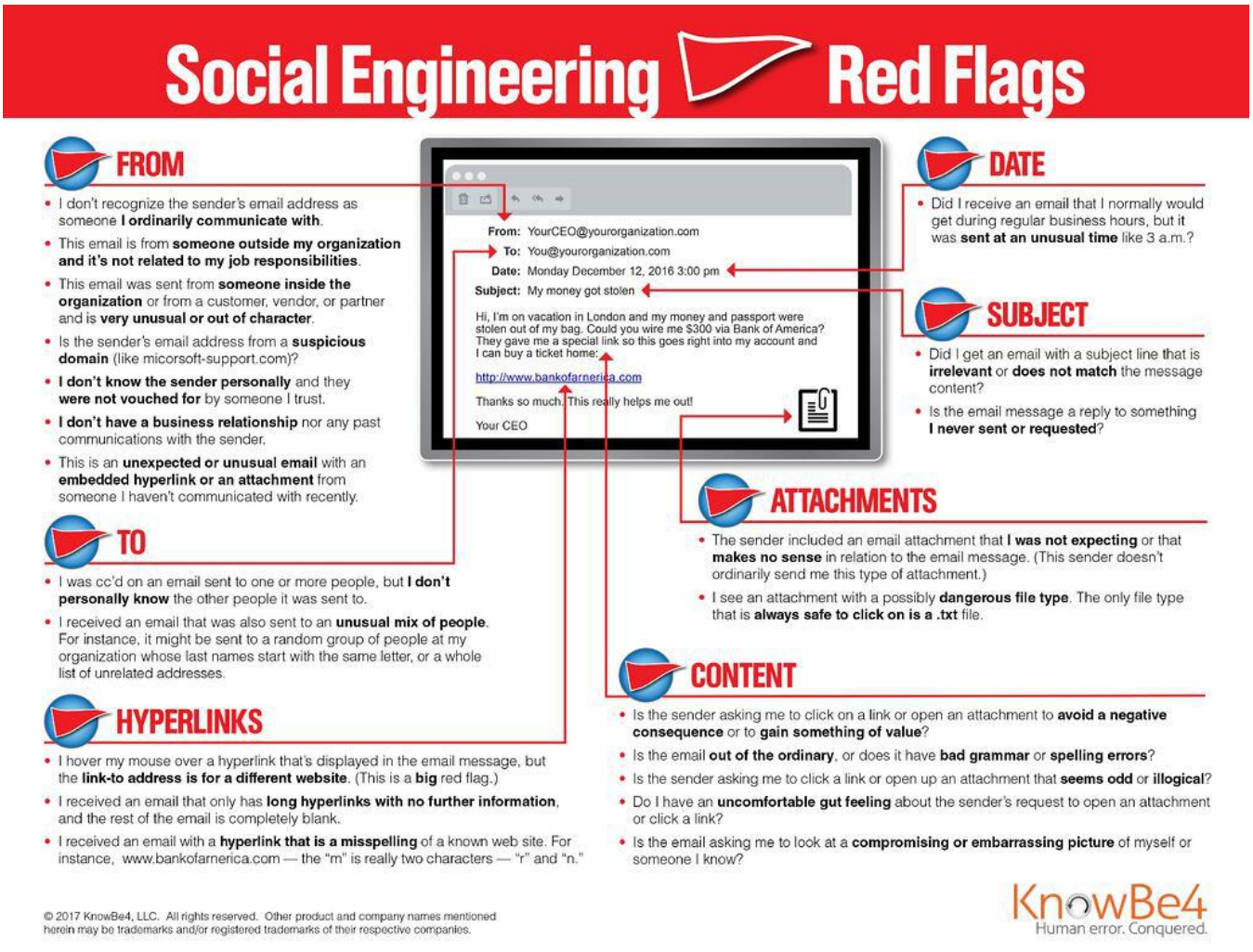
Usually carried out over email - although the scam has now spread beyond suspicious emails to phone calls (so-called 'vishing') social media, messaging services (aka 'smishing') and apps - a basic phishing attack attempts to trick the target into doing what the scammer wants.

Why is phishing called phishing?

The overall term for these scams -- phishing -- is a modified version of 'fishing' except in this instance the one doing this fishing is the crook, and they're trying to catch you and reel you in with their sneaky email lure.

It's also likely a reference to hacker history: some of the earliest hackers were known as 'phreaks' or 'phreakers' because they reverse engineered phones to make free calls.

The first phishing lawsuit was filed in 2004 against a Californian teenager who created the imitation of the website “America Online”. With this fake website, he was able to gain sensitive information from users and access the credit card details to withdraw money from their accounts.



Common Features of Phishing Emails

1. **Too Good To Be True -** Lucrative offers and eye-catching or attention-grabbing statements are designed to attract people's attention immediately. For instance, many claim that you have won an iPhone, a lottery, or some other lavish prize. Just don't click on any suspicious emails. Remember that if it seems to good to be true, it probably is!
2. **Sense of Urgency -** A favorite tactic amongst cybercriminals is to ask you to act fast because the super deals are only for a limited time. Some of them will even tell you that you have only a few minutes to respond. When you come across these kinds of emails, it's best to just ignore them. Sometimes, they will tell you that your account will be suspended unless you update your personal details immediately. Most reliable organizations give ample time before they terminate an account and they never ask patrons to update personal details over the Internet. When in doubt, visit the source directly rather than clicking a link in an email.
3. **Hyperlinks -** A link may not be all it appears to be. Hovering over a link shows you the actual URL where you will be directed upon clicking on it. It could be completely different or it could be a popular website with a misspelling, for instance www.bankofarnerica.com - the 'm' is actually an 'r' and an 'n', so look carefully.
4. **Attachments -** If you see an attachment in an email you weren't expecting or that doesn't make sense, don't open it! They often contain payloads like ransomware or other viruses. The only file type that is always safe to click on is a .txt file.
5. **Unusual Sender -** Whether it looks like it's from someone you don't know or someone you do know, if anything seems out of the ordinary, unexpected, out of character or just suspicious in general don't click on it!

Prevent Phishing Attacks:

Though hackers are constantly coming up with new techniques, there are some things that you can do to protect yourself and your organization:

- To protect against spam mails, spam filters can be used. Generally, the filters assess the origin of the message, the software used to send the message, and the appearance of the message to determine if it's spam. Occasionally, spam filters may even block emails from legitimate sources, so it isn't always 100% accurate.
- The browser settings should be changed to prevent fraudulent websites from opening. Browsers keep a list of fake websites and when you try to access the website, the address is blocked or an alert message is shown. The settings of the browser should only allow reliable websites to open up.
- Many websites require users to enter login information while the user image is displayed. This type of system may be open to security attacks. One way to ensure security is to change passwords on a regular basis, and never use the same password for multiple accounts. It's also a good idea for websites to use a CAPTCHA system for added security.
- Banks and financial organizations use monitoring systems to prevent phishing. Individuals can report phishing to industry groups where legal actions can be taken against these fraudulent websites. Organizations should provide security awareness training to employees to recognize the risks.
- Changes in browsing habits are required to prevent phishing. If verification is required, always contact the company personally before entering any details online.
- If there is a link in an email, hover over the URL first. Secure websites with a valid Secure Socket Layer (SSL) certificate begin with "https". Eventually all sites will be required to have a valid SSL.

Phishing

WHAT YOU NEED TO KNOW

SCAMMERS ARE AFTER YOUR

Passwords | Financial Info | Identity | Money

WHY DO WE FALL FOR THESE SCAMS?

- Urgency
- Desire to please
- Greed
- Curiosity
- Complacency
- Fear

PROBABILITY THAT A PHISHING MESSAGE SUCCEEDS

1 out of 10!

WATCH OUT FOR

- Spelling & Grammar Errors
- Sender Address
- Things That Sound Too Good to be True

BEWARE OF UNSOLICITED MESSAGES

- Attachments
- Links
- Login Pages

IF YOU SEE SOMETHING, SAY SOMETHING!

Report phishing emails to spam@stanford.edu

security.stanford.edu

Generally, emails sent by a cybercriminals are masked so they appear to be sent by a business whose services are used by the recipient. A bank will not ask for personal information via email or suspend your account if you do not update your personal details within a certain period of time. Most banks and financial institutions also usually provide an account number or other personal details within the email, which ensures it's coming from a reliable source.

Phishing Example:

Subject: Important Update

From: IRS Service <irs@services.com(link sends e-mail)>

Date: 1/15/2016 2:58 PM

To: "<"<irs@services.com(link sends e-mail)>

As we prepare to start the 2016 Tax filling season, we have undergone slight changes in the filling process to make filling for your refund easier and to prevent unnecessary delays. Part of the changes include updating our database with your

information.
Please ensure to carefully complete this verification to avoid hitches in processing your refund.
We have sent you an attachment, open it and follow the steps to verify your profile.

Here is a great KnowBe4 resource that outlines 22 social engineering red flags commonly seen in phishing emails. We recommend printing out this PDF to pass along to family, friends, and coworkers.
https://cdn2.hubspot.net/hubfs/241394/Knowbe4-May2015-PDF/SocialEngineeringRedFlags.pdf?t=1490956890483