SERC Reliability Corporation

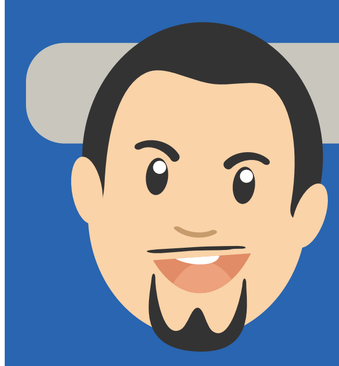
HOW TO SPOT A PHISH

FINDING THE PHISH 101

with Captain Ike

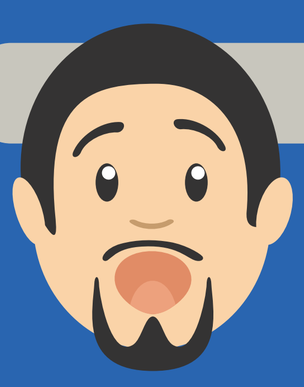
December 2015 over 700,000 customers lost power in Ukraine due to a phishing attack.

LESSON #1: WATCH OUT FOR EMOTIONS



GREED

Phishing emails often dangle a financial reward of some kind if you click a link or enter your login information. If an email offers you something that seems too good to be true, it probably is.

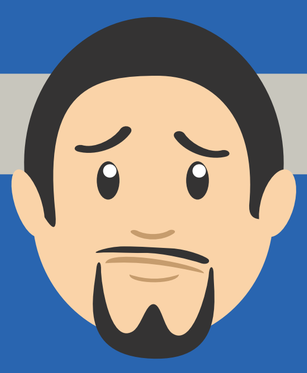


URGENCY

If an email provides a strict deadline for performing an action -- be suspicious. Phishing emails will try to fluster recipients by creating a sense of urgency.

CURIOSITY

People are naturally curious, and phishers take advantage of this by sending emails that promise to show us something exciting or forbidden.



FEAR

Scaring recipients is a common tactic in phishing emails. Emails that threaten you with negative consequences or punishment should be treated with suspicion.

LESSON #2: EXAMINE THESE ITEMS CLOSELY

EMAIL SIGNATURES

A signature block that is overly generic or doesn't follow company protocols could indicate that something is wrong.

SENDER ADDRESS

If the address doesn't match the sender name, be suspicious of the entire email.

EMAIL TONE

We know how our co-workers and friends talk, so if an email sounds strange, it's probably worth a second look.

LESSON #3: BEWARE OF THESE ELEMENTS

From: Kevin Smith
To: Captain Ike
Subject: WebMail Migration

Attachment - WebMail_Migration.pdf

ATTACHMENTS
When an attachment comes from someone you don't know or if you were not expecting the file, make sure it's legitimate before opening it.

Captain Ike,
This email is to inform you that we are in the process of migrating our email infrastructure to the ne a password.

LOG-IN PAGES
Spear phishers will often forge login pages to look exactly like the real thing in order to steal your credentials.

Attached is a document outlining the benefits of the migration. We request you enter your Windows password before 10PM on Monday. Failure to do so will result in being locked out of your email account.

Pease click here to update your password.

Thank You,
Kevin Smith

LINKS
Roll your mouse pointer over the link and see if what pops up matches what is in the email. If they do not match, do not click.

IF YOU SEE SOMETHING, REPORT IT!

Phish Alert

Report suspected phishing emails to the information security team.

SERC Reliability Corporation

THE STORY OF A PHISH

STORY BEGINS HERE

MEET CAPTAIN IKE

Captain Ike works for a local utility company.

91% of cyber-attacks begin with spear phishing

HE STARTS EVERY MORNING BY CHECKING HIS EMAIL.

16% Averge click rate for the utility industry with phishing emails

121 EMAILS Average number of emails an office worker receives each day

At 10:00 a.m., Captain Ike walks to the cafeteria for his daily latte & bagel.

WHILE HE'S WAITING FOR HIS LATTE HE CHECKS FACEBOOK ON HIS CELL PHONE.

Hackers access credentials and research social media profiles to gain intelligence about people they're targeting. Their goal is to build highly personalized 'lures' that are likely to be opened.

1.6 BILLION people use Facebook

Dangerous mobile apps from rouge marketplace affect 2 in 5 enterprises

25% of Facebook users do not use privacy settings

20% of social media users set their profile to completely public

In 2015, social media engineering was the #1 attack technique. People replaced exploits as attackers' favorite way to beat cybersecurity

BACK AT HIS DESK, CAPTAIN IKE DISCOVERS HE AMASSED 40 WORK EMAILS WHILE HE WAS AWAY.

He quickly runs through them not paying any attention to where he is clicking.

23% of the recipients now open phishing messages

One in 5 clicks on malicious URLs occured off the network, many of them from social media and mobile devices

11% click on attachments

HE GETS A TEXT FROM HIS WIFE AMMY, REMINDING HIM ABOUT DINNER WITH THE NEIGHBORS THAT NIGHT.

Ammy works as an HR manager for local technology company.

1 in 1000 devices are infected with mobile surveillance and Mobile Remote Access Trojans (MRATS)

One email catches his eye. It appears the company is holding a series of training sessions to help employees avoid phishing attacks.

HE DELETES THE EMAIL. HE IS NOT CONCERNED, AS HIS COMPUTER HAS ANTI-VIRUS AND ANTI-SPAM SOFTWARE.

70% of critical infrastructure companies suffered a security breach over the last year

Demand for US information security professionals is expected to grow by **53%** through 2018

Anti-spam is NOT 100% effective. Not even anti-spam vendors claim 100% effectiveness

95% of web apps attacks involved harvesting credentials stolen from customer devices, then logging to web apps with them

HE CLICKS ON AN EMAIL THAT APPEARS TO BE FROM A REPUTABLE UTILITY ORGANIZATION.

Captain Ike has now unknwingly fallen victim to a phishing scam.

The most effective phishing emails contain business communication theme:

36% opened with "File from Scanner"

and

34% opened with "Unauthorized Activity Access"

THE AFTERMATH

CYBERCRIME WILL COST BUSINESSES OVER $2 TRILLION BY 2019

The forecast average loss for breach of 1,000 records is between **$52,000 and $87,000**

People remain the weakest link in security

38% of spear phishing targets companies with 250 or less employees

SERC Reliability Corporation

PHISHING AND SOCIAL MEDIA

MILLIONS of people log in to their social media profiles every day.

Captain Ike is just one social media user of many. He logs on to share his photos and to check up on his friends.

1,600,000,000

In fact, over 1.6 billion users like Captain Ike log onto their favorite social networking sites monthly.

ON HIS PROFILE, YOU CAN FIND:

Name, Date of Birth, Location, Workplace, Interests, Hobbies, Skills, Relationship Status, Telephone Number Email Address and Favorite Food

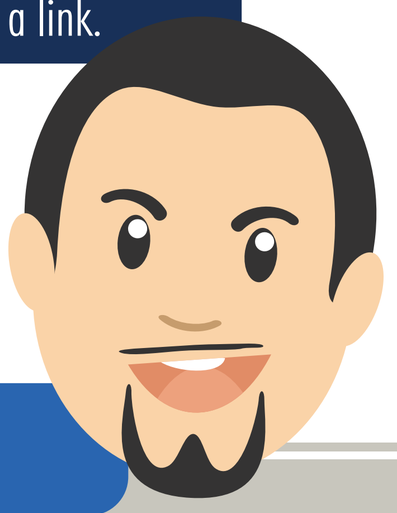
ALL of this information can be used against Captain Ike by social engineers.

SO·CIAL EN·GI·NEER·ING

In spear phishing, social engineering is the use of known social behaviors and patterns to make targets more likely to take a suggested course of action, e.g. clicking on a link.

They can send crafted spear phishing emails to Captain Ike's inbox...

...or they can imitate Captain Ike to trick his contacts.



SOCIAL MEDIA USAGE BY THE NUMBERS

66% of adult Facebook users do not know how to use its privacy controls

9% of teenage social media users even have concerns about the privacy of their data

OVER 75% of all Internet users use social media.

18–49 YEARS OLD in this age group, YouTube has greater reach than any cable network

LUCKILY, THERE ARE WAYS TO KEEP YOUR INFORMATION SAFE!

Be cautious when you receive suspicious messages from your contacts - old or new.

Remember that all information can be stolen from your photos as well as from text.

Don't submit status updates you wouldn't want on the front page of the newspaper.

- [x] **YOU CAN INCREASE YOUR PRIVACY SETTINGS SO ONLY FRIENDS CAN SEE YOUR PROFILE.**
- [x] **BE CAREFUL WHAT WEBSITES YOU LINK YOUR PROFILES TO.**

40% of Facebook accounts and 20% of Twitter accounts claiming to represent a fortune 100 Brand are UNAUTHORIZED

DID YOU KNOW?

- One major social network has more fake profiles than the population of Egypt
- Social activities account for 91% of all mobile internet activity
- Web users found that 77% use Facebook, 63% use YouTube, 25% use LinkedIn, 24% use Google Plus, and 21% use Twitter