SALFORD & CO.

HOME ABOUT CONTACT

PHISHING

ABDULLAH HIMAYAT ALI

tiwari786sahab

INTRODUCTION TO PHISHING

DEFINITION: PHISHING IS A CYBER ATTACK WHERE ATTACKERS IMPERSONATE LEGITIMATE ORGANIZATIONS OR INDIVIDUALS TO TRICK VICTIMS INTO PROVIDING SENSITIVE INFORMATION SUCH AS PASSWORDS, CREDIT CARD NUMBERS, OR PERSONAL DATA.

GOAL: RAISE AWARENESS ABOUT PHISHING ATTACKS, RECOGNIZE PHISHING ATTEMPTS, AND PROTECT AGAINST THEM.

TYPES OF PHISHING ATTACKS

- EMAIL PHISHING: FAKE EMAILS THAT LOOK LIKE THEY COME FROM TRUSTED SOURCES.
- SPEAR PHISHING: TARGETED PHISHING AIMED AT A SPECIFIC INDIVIDUAL OR ORGANIZATION.
- CLONE PHISHING: REPLICATES LEGITIMATE EMAILS BUT WITH MALICIOUS LINKS OR ATTACHMENTS.
- VISHING: VOICE PHISHING, WHERE ATTACKERS USE PHONE CALLS TO TRICK PEOPLE.
- SMISHING: PHISHING ATTACKS USING SMS MESSAGES TO COLLECT PERSONAL INFORMATION.
- PHARMING: REDIRECTS USERS FROM LEGITIMATE WEBSITES TO FAKE ONES TO STEAL INFORMATION.

COMMON PHISHING EMAIL CHARACTERISTICS

- GENERIC GREETINGS: "DEAR CUSTOMER" INSTEAD OF USING YOUR NAME.
- URGENT LANGUAGE: "IMMEDIATE ACTION REQUIRED" OR "YOUR ACCOUNT WILL BE CLOSED."
- SUSPICIOUS ATTACHMENTS: UNSOLICITED FILES, WHICH COULD CONTAIN MALWARE.
- SPOOFED LINKS: LINKS THAT SEEM LEGITIMATE BUT LEAD TO A FRAUDULENT SITE.
- MISMATCHED URLS: HOVERING OVER A LINK REVEALS A DIFFERENT DESTINATION.

HOW TO RECOGNIZE PHISHING WEBSITES

- CHECK THE URL: LOOK FOR MISSPELLED DOMAINS OR EXTRA CHARACTERS (E.G., WWW.GOOGLE.COM).
- UNSECURE WEBSITE: NO HTTPS PADLOCK IN THE BROWSER'S ADDRESS BAR.
- DESIGN FLAWS: POOR WEBSITE LAYOUT OR INCONSISTENT BRANDING.
- REQUESTS FOR SENSITIVE INFORMATION: LEGITIMATE WEBSITES RARELY ASK FOR SENSITIVE DETAILS (PASSWORDS, SSN, ETC.) OVER EMAIL OR POP-UP FORMS.
- TOO GOOD TO BE TRUE OFFERS: WEBSITES OFFERING UNREALISTIC DEALS.

UNDERSTANDING SOCIAL ENGINEERING

- WHAT IS SOCIAL ENGINEERING?: MANIPULATING PEOPLE INTO BREAKING NORMAL SECURITY PROTOCOLS TO GAIN ACCESS TO SYSTEMS OR CONFIDENTIAL INFORMATION.
- EXAMPLES:
- PRETEXTING: IMPERSONATING SOMEONE TO GAIN INFORMATION (E.G., IT SUPPORT ASKING FOR LOGIN CREDENTIALS).
- BAITING: OFFERING SOMETHING ENTICING, LIKE FREE SOFTWARE, THAT LEADS TO MALWARE.
- TAILGATING: GAINING UNAUTHORIZED ACCESS TO SECURE AREAS BY FOLLOWING SOMEONE WHO HAS ACCESS.

HOW TO PROTECT YOURSELF FROM PHISHING ATTACKS

- VERIFY THE SOURCE: DOUBLE-CHECK THE SENDER’S EMAIL ADDRESS AND ANY LINKS BEFORE CLICKING.
- USE STRONG, UNIQUE PASSWORDS: USE DIFFERENT PASSWORDS FOR DIFFERENT SERVICES AND ENABLE TWO-FACTOR AUTHENTICATION (2FA).
- UPDATE SOFTWARE REGULARLY: ENSURE YOUR SYSTEM AND APPLICATIONS ARE UP TO DATE WITH SECURITY PATCHES.
- THINK BEFORE YOU CLICK: BE CAUTIOUS ABOUT OPENING ATTACHMENTS OR CLICKING LINKS, EVEN FROM KNOWN SOURCES.
- BE SKEPTICAL OF URGENT REQUESTS: TAKE TIME TO ASSESS IF A REQUEST IS LEGITIMATE.
- REPORT PHISHING ATTEMPTS: USE YOUR EMAIL PROVIDER'S "REPORT PHISHING" FEATURE OR CONTACT YOUR ORGANIZATION'S IT TEAM.

WHAT TO DO IF YOU SUSPECT A PHISHING ATTACK

- DON’T CLICK: AVOID INTERACTING WITH SUSPICIOUS EMAILS OR WEBSITES.
- REPORT IT: FORWARD THE PHISHING ATTEMPT TO YOUR IT DEPARTMENT OR USE ONLINE REPORTING TOOLS.
- CHANGE PASSWORDS: IF YOU’VE FALLEN VICTIM, CHANGE YOUR PASSWORD IMMEDIATELY AND REVIEW YOUR ACCOUNT FOR SUSPICIOUS ACTIVITY.
- MONITOR ACCOUNTS: KEEP AN EYE ON BANK AND ONLINE ACCOUNTS FOR UNAUTHORIZED ACTIVITY.

CASE STUDY: REAL-LIFE PHISHING ATTACK

- FACEBOOK AND GOOGLE (€90 MILLION)
- BETWEEN 2013 AND 2015, TWO OF THE WORLD'S BIGGEST TECH FIRMS WERE DUPED OUT OF $100 MILLION (ABOUT €90 MILLION AT THE TIME) AFTER FALLING VICTIM TO A FAKE INVOICE SCAM.
- A LITHUANIAN MAN, EVALDAS RIMASAUSKAS, NOTICED THAT BOTH ORGANISATIONS USE THE TAIWANESE INFRASTRUCTURE SUPPLIER QUANTA COMPUTER.
- HE SENT A SERIES OF BOGUS MULTIMILLION-DOLLAR INVOICES REPLICATING THE SUPPLIER OVER TWO YEARS, COMPLETE WITH CONTRACTS AND LETTERS THAT APPEARED TO HAVE BEEN SIGNED BY EXECUTIVES AND AGENTS OF FACEBOOK AND GOOGLE.
- THE SCAM WAS EVENTUALLY DISCOVERED, AND FACEBOOK AND GOOGLE TOOK LEGAL ACTION. THEY RECOVERED JUST UNDER HALF OF THE STOLEN MONEY, WHILE RIMASAUSKAS WAS ARRESTED AND EXTRADITED FROM LITHUANIA.

IN DECEMBER 2019, HE WAS SENTENCED TO FIVE YEARS IN PRISON.

CONCLUSION & KEY TAKEAWAYS

- PHISHING IS ONE OF THE MOST COMMON AND DANGEROUS CYBER THREATS.
- STAYING VIGILANT, RECOGNIZING SIGNS, AND ADOPTING BEST PRACTICES CAN PREVENT PHISHING ATTACKS.
- REGULAR TRAINING AND AWARENESS ARE KEY TO PROTECTING PERSONAL AND ORGANIZATIONAL INFORMATION.

SOURCES

- HTTPS://WWW.ITGOVERNANCE.EU/BLOG/EN/THE-5-BIGGEST-PHISHING-SCAMS-OF-ALL-TIME
- HTTPS://CONSUMER.FTC.GOV/ARTICLES/HOW-RECOGNIZE-AND-AVOID-PHISHING-SCAMS
- HTTPS://WWW.PHISHING.ORG/WHAT-IS-PHISHING

THANK YOU