SPEAR PHISHING: WHAT YOU NEED TO KNOW ABOUT THIS SERIOUS SECURITY THREAT

UNDERSTANDING SPEAR PHISHING

What is phishing/spear phishing?

PHISHING is a type of fraudulent activity in which an attacker tries to acquire sensitive or confidential information such as user names, passwords, banking or credit card details, by posing as a reputable company or person.

SPEAR PHISHING is a phishing technique that is **specifically targeted at you** in an attempt to obtain valuable information. Typically performed by an individual or small group of people, it is usually in the form of an email message that is designed to look completely legitimate but is actually impersonating a known and trusted person. Spear phishers may even go so far as to research company websites and social media platforms to learn key stakeholder names, titles, and writing styles to seem more credible.

> Spear phishers may even go so far as to research company websites and social media platforms to learn key stakeholder names, titles, and writing styles to seem more credible.

What is the goal of a spear phishing attempt?

Criminals who engage in spear phishing are ultimately after financial gain. They accomplish this in many ways, most notably by stealing:

- Access to sensitive financial information
- User IDs and passwords
- Access to your company's computer network
- Intellectual property

How do they achieve this?

Spear phishing victims are tricked into clicking on a **malicious link**, opening a **malicious email attachment**, or simply **replying to a message** with the requested valuable information.

It is not uncommon to see a spear phishing message that appears to be from a high ranking executive within your company, requesting important financial data like wiring instructions, bank account details, or account credentials.

> It is not uncommon to see a spear phishing message that appears to be from a high ranking executive within your company, requesting important financial data.

HOW TO SPOT A SPEAR PHISHING ATTEMPT

1. **FORGED EMAIL ADDRESSES:** The email address may look valid, but it could be a forgery. To determine email address validity, compare the sender's email display name to the sender's email address and domain name to see if they match. Other times, you may need to examine the Internet headers associated with the email to determine the name of the email server that actually sent the message. **Check with your IT department for procedures on locating the Internet headers for your email client.**

2. **FORGED HYPERLINKS:** The hyperlink may look valid, but it could be a forgery. With your mouse, hover over the link to see if it matches what appears in the text of the email, but **be very careful not to click on the link!** Also keep an eye out for typos or incorrect grammar and punctuation. This is often a tell-tale sign of spear phishing.
3. **REQUESTS FOR SENSITIVE INFORMATION**: Is there a URL link or request for banking information included in the email? Think twice before clicking or replying; it is most likely a phishing attempt. It's always better to open a new browser window and directly type in the URL for your bank or call your bank if you are still unsure.
4. **PUBLIC INFORMATION:** The sender seems to know a lot about you and your business, but much of that information may be accessible publicly through your company website, social media profiles and even in news stories.
5. **EMAIL TONE:** Does the cadence, tone, and writing style of the email from your colleague or contact sound correct? If the words they are using seem a bit off or the tone is curt, it's best to double-check the email's validity.
6. **SENSE OF URGENCY:** Does the email sender threaten to shut down access to your account unless you act fast? This is a huge red flag of a phishing attempt.
7. **"OUT OF THE BLUE" REQUESTS:** You should always ask yourself, "Does this person usually request this type of information?" or "Does this person really need this information to do their job?"

Ask yourself: "Does this person usually request this type of information?" or "Does this person really need this type of information to do their job?"

WHY YOU SHOULD BE CONCERNED

SPEAR PHISHING WORKS: Spear phishing email attacks have an **open rate of 70%,** compared to the traditional phishing open rate of just 3%.

THE LOSSES ARE MUCH HIGHER: The average financial return from each spear phishing victim is **40 times more** than that of regular phishing.

WHAT YOU CAN DO TO PROTECT YOUR COMPANY

- **COMMUNICATE** these increased risks to all employees involved with the sharing of financial information or the transferring of funds.
- **CHANGE** the way funding/wire/money transfer requests are made: (e.g.) Verbal requests instead of email; Dual approvals.
- **LIMIT** the number of employees authorized to make or approve fund transfers.
- **UTILIZE** out-of-band authentication and one-time PINS.
- **DISCUSS** with your IT department if there are any additional security measures that can be taken to reduce the risk of spear phishing.
- **DEPLOY** an email threat detection platform such as Agari Enterprise Protect, which uses proprietary global email telemetry data to detect low-volume, targeted email attacks that go undetected by existing email security systems.

More information on spear phishing can be found here:
Spear Phishing Attacks – Why They Are Successful and How to Stop Them (FireEye)
Top 5 Reasons to Re-Examine Your Email Security Solutions (FireEye)
Email Attacks: This Time It's Personal (Cisco)