DEEP DIVE INTO CYBER

Explore the targeted techniques used by cybercriminals

THIS MONTH'S TOPICS:

Spear Phishing

Understanding the risks...

Search Engine Results

Compare these three results...

Scam of the Month:

Document Replacement Scams...

The Monthly Mashup:

Cybersecurity Awareness Month Prep...

Phishing and fishing have a lot in common. Many cybercriminals opt for generic, mass phishing messages which give them a larger group of fish to catch. However, to catch particular fish, sometimes you must use specific bait and techniques.

By creating customized spear phishing attacks and targeted websites that show up in search engine results, cybercriminals are hooking us before we think twice about questioning it.

In this month's newsletter, learn more about customized scams and the way cybercriminals take advantage of particular topics and situations.

Spear Phishing

Just like fishing, phishing often requires a targeted attack in order to catch a specific fish. In the cybersecurity world, these attacks are known as spear phishing.

Spear Phishing: A type of social engineering attack that targets a specific user by utilizing their personal information in a message. This type of scam often mimics emails from senders who the user already trusts.

Commonly Used Personal Information:

- Name
- Place of work
- Birth date
- Previous orders and interests
- Names of friends, family, or coworkers

EXAMPLE

Cybercriminals use information on the dark web or from social media to craft customized messages like this:

www.gmail.com

LS Linda Smith <lsmith40602867@gmail.com>

Hello Gary,

I'm in a meeting and need you to help me with a task. Could you please resend me your cell #?

Linda Smith, CEO of Your Company

Key Takeaways

-Just because a message has a familiar name, doesn't mean it is real.

-Be wary of out of the blue requests.

-Keep personal details off of social media when possible.

Deep Dive

Search Engine

RESULT ANALYSIS

Best place to vacation this year

THE PERSONAL BLOG

mandytravels.net

- Unknown website, possibly not secure.
- Likely has many advertisements, pop ups, and affiliate links.
- Might not be as unbiased as an official website.

OFFICIAL NEWS WEBSITE

forbes.com/travel

- Legitimate, well-known company.
- Naturally listed at the top of search result, unlike sponsored ads.
- Confirm the URL matches the real company before clicking.

SPONSORED ADVERTISEMENT

vtravl.ot2.xrl.com

- Suspicious website URL.
- Sponsored ads mean they aren't naturally top search results.
- Unknown company with vague name.

Turtle Tip

Examine website names and URLs closely before clicking anything.

SCAM OF THE MONTH

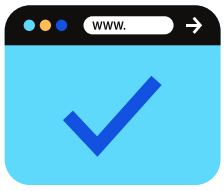
Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

In the aftermath of a devastating flood, Adriana found herself grappling with the loss of her family's belongings and important documents. She stumbled upon an online advertisement promising quick and hassle-free document replacement services. Intrigued and desperate to regain some sense of normalcy, Adriana clicked on the link that led her to a seemingly legitimate website. The site, adorned with reassuring testimonials and professional graphics, convinced her that they could swiftly replace all her lost documents for a reasonable fee. Adriana provided her personal information and credit card details, believing she had finally found a solution to her problems.

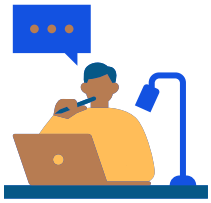
Days turned into weeks, and Adriana still had not received her documents or any updates from the supposed service. It wasn't until a friend shared a news article about fraudulent disaster relief websites that Adriana realized the documents were not coming, and she had been scammed.

Did you spot the red flags?

- In her desperation and hurry to obtain the documents she had lost, Adriana clicked on the first website she saw, instead of researching and reading reviews.
- The website promised quick document replacement for a fee. Many government agencies will replace documents for free after an emergency.



Verify URLs and phone numbers before giving any information to a company. Many scammers use look alike websites or phone numbers.



While there are some legitimate third-party websites that help with document replacement, make sure to research and read reviews first.

Even if you were not impacted by a natural disaster, be on the lookout for these scams. Scammers often text or call and say you need to replace your Medicare card, Social Security card, or driver's license. Always go to official agency websites and verify their phone number or go in person.

THE MONTHLY MASHUP

KEY TAKEAWAYS

There are many ways cybercriminals try to get users to act without thinking. In times where you are fatigued or rushed, try to take a quick pause before acting and think about your training.

CYBERSECURITY AWARENESS MONTH CHECKLIST

Cybersecurity Awareness Month starts October 1st! Make sure you are prepared by following this checklist.

- [ ] **Start using a Password Manager.**
- [ ] **Update software on all devices.**
- [ ] **Review the SLAM method for identifying phishing messages.**
- [ ] **Enable Multi-Factor Authentication on all accounts that offer it.**