



CYBER SECURITY MONTH



Phishing

Christina Belfiglio

October 2021

What is Phishing

According to Phishing.org, phishing is defined as “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.

The information is then used to access important accounts and can result in identity theft and financial loss.”

Phishing is not a lost sport

Phishing attacks account for more than 80% of reported security incidents. The attacks can come in the form of emails, phone calls, text messages or chat boxes.

Some common features of phishing messages:

- Spoofed Email address
- Email is addressed to a general audience such as “Dear Customer” or “Friend”
- Poor grammar and/or spelling
- Sense of Urgency
- Email contains links or attachments

Below is an example which contains several key indicators that this message is a scam, such as:

1. The sender’s name has no association with the email address. The email address does not list a company name.
2. The email has been addressed to “friend” instead of directly to the recipient.
3. There is poor grammar throughout the email.
4. The email provides a link which does not indicate a company name.
5. At no point does the sender indicate the company they are promoting.

1 Matthew Carey <scroll5038@earthlink.net>

Fri 9/3/2021 5:23 PM

To: You

2 friend are you someone who's in need of a work at this time?

3 Are you currently in need of a good source of earn-ings that will not require lots of effort from you?

I am Matthew Carey and want to discuss with you about the things that I can provide you with.


I am here in order to provide you home-working types of job offers friend that can be the solution to all your problems.


4 Just go to <https://tinyurl.com/yfobtqj4> and see all the job offers which one can get as you select to remain at home.

Never demanding, hassle free and pays more than enough - that is the kind of job that you will get if you choose to find out more.

5 Matthew Carey

What to do if you responded to a phishing message:

 If you think a scammer has your information, like your social security, credit card, or bank account numbers go to [IdentityTheft.gov](https://www.identitytheft.gov). The website provides resources for many scenarios.

 If you clicked on a link or opened an attachment that may be harmful update your computer security software, then run a scan.



Safeguard your Private Information

New Phishing Bait:

Fraudsters are no longer relying on emails alone for their schemes. Phone calls and text messages are also used to obtain logins, passwords, and other personal information. Typically, the scammer sends a text message to the potential victim asking if they made a specific purchase. If the victim responds, “No,” the scammer calls the victim claiming to be the vendor or financial institution and asks for sensitive information.

Report Phishing:

- ✉ Forward phishing emails to Anti-Phishing Working Group at reportphishing@apwg.org
- ✉ Forward phishing text messages to SPAM (7726)
- ✉ Report Phishing attacks to the FTC at [ReportFraud.ftc.gov](https://www.ftc.gov/ReportFraud)

How you can protect yourself:

- 🔒 Install anti-virus software on your computer, phone, and other electronics
- 🔒 Consider a password management app to help you remember your login credentials and security questions/answers. These apps can create strong passwords that are very difficult to guess.
- 🔒 Consider answering security questions with a different answer.
- 🔒 Do not click on links in text messages or emails. Go directly to the known website to log in.
- 🔒 Never provide personal information or login credentials to someone who calls you. Instead, call the main number of the institution and explain the situation so they can verify if the call was legitimate and transfer you to the correct department.

“Amateurs hack systems, professionals hack people.” Bruce Schneier

Sources:

<https://www.phishing.org/what-is-phishing>

<https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>

<https://www.schwab.com/resource-center/insights/content/beware-next-level-phishing?cmp=em-RBL>