Phishing 101

Have you ever imagined that scanning a single QR code would result in stealing your credentials? Or simply listening to a voicemail could result in your money getting stolen? Sounds illogical but it's true, and many people fall for it to this day. The two mentioned acts fall under what goes by the name "Phishing". So, what exactly is phishing, what are its types, and how to protect ourselves from it?

Phishing is a type of scam that comes in different forms such as - and not limited to - email, phone, SMS, and social media. The main goal of phishing is to trick you into revealing sensitive information such as passwords, credit card numbers, and OTPs (one-time passwords). It may also trick you into download malicious files on your device that also work on stealing your confidential data and files! In this module, we'll discuss the types of phishing attacks that you should be aware of in order to protect yourself from such attacks.

1- **Email Phishing**

   "Suspicious account activity detected, click here to protect your account". An innocent mail trying to "protect" your account telling you to click a link to "secure" your account. Seems legit, right? That's how attackers get to you: URGENCY. They frighten you up by telling you that your

account is compromised and you need to act fast, or lure you into thinking you have won a prize and requesting from you to go to a specific website to claim your prize before it's too late.

Back in 2013 to 2015, a man named Evaldas Rimasauskas managed to trick BOTH Facebook (now Meta) and Google into wiring him over $100 million! The technique he used is email phishing. What he did was impersonate a genuine Taiwanese electronics manufacturer Quanta Computer, that was a known business associated with both companies, and send fake invoices via email which both companies kept paying over the span of two years. Isn't that quite surprising?

2- Smishing and Vishing

Did it ever occur to you that out of nowhere, one of your friends on Facebook messaged you saying that they're in desperate need of some money? Or even better: they send you a voice note instead of a normal text message so it sounds more believable! That's what smishing and vishing are. Smishing refers to an attacker impersonating one of your friends via text, while vishing is the same but via voice. It can come from a fake account impersonating one of your friends, or from your own friend's account if their account is compromised.

Smishing and Vishing is not only limited to social media, it can come in the form of SMS texts from your bank, or to be more precise, someone impersonating your bank telling you

that your credit card is getting deactivated soon and you need to call them to prevent that from happening. They could also trick you into sharing your OTP code that gives them access to your account or authorizes a money transaction. Attackers are getting smart with their techniques every day, so better stay aware!

3- Quishing

You probably heard about the dangers of unknown links and the malicious stuff they could do. But what if I told you that Quishing (short for QR code phishing) is almost the same but you're unaware of it? Many restaurants adapted to using QR codes to showcase their menu, other organizations use them to ease access to their websites by simply scanning the QR code instead of typing the website into the browser manually, others use it for surveys and forms filling, it has many usages.

Attackers make use of quishing to lure you into their malicious websites or download malware. They can craft a QR code, print it on paper, and stick it on a wall next to a restaurant. You'd think that this QR code belongs to the restaurant, so you scan it innocently, only to be surprised that you visited a malicious link. You could also find those type of QR codes on social media, they share a QR code claiming it's an entry to a contest or a giveaway, to which you visit the link and insert your credentials, only to find out they're stealing them. Creativity never stops, nor do attackers.

Phishing is widely used by attackers to gain sensitive information or data from victims. While it's effective on most, you can still protect yourself from such attack.

1- **Avoid Clicking Random Links:** Not every email you receive is safe. An email claiming they're Facebook and urging you to change your password? Check the link to see if it actually belongs to Facebook or not. Received a link from an unknown source? Don't bother to click it, ignore it and move on with your day. It's preferable not to click any link you receive, but sometimes you have to, as long as it's legit.

2- **Enable 2FA:** 2FA, or Two-Factor Authentication, adds an extra layer of security to your accounts. Even if an attacker got your email and password through a phishing attack, with 2FA enabled, they still can't access your account. 2FA requires you to insert an OTP (One-Time passcode) sent to your phone number or email in order to get into your account.

3- **Verify Communications:** If your friend really needs money, they most likely would call you from their phone number and not message you on Facebook or social media in general. Thus, if it happens that they send you a message on social media, call them on their phone number and check if it was them who sent the message or not. Attackers can use AI to impersonate the voice of your friend even on a call, but still they would most likely use a different phone number from that of your friend's.

4- **Avoid ‘too good to be true’ situations:** Free subscription to Netflix? An iPhone giveaway for no apparent reason? A free entry to win one million dollars? All of these are too good to be true, which means they’re most likely fake. Don’t believe anything you see or receive online, most of them are scams with the sole purpose of stealing your data and confidential information.

5- **Check Sources:** Check that the message you received comes from an authentic source. An email claiming they’re Facebook telling you to reset your password. Is the mail coming from the authentic email address of Facebook, or a random unknown email address? A quick google search would help you identify the official email address of Facebook, simply search “Official Facebook Email Address”. Same goes for other organizations, whether it’s email address, phone number, or any other form of communication.