フィッシングに釣られるな！

【物語編】

■それぞれの部屋

Limeグループ通話（音声のみ）で雑談をしている3人。佳乃と春菜はPCの前にいる。

亮「昨日、うちの母さんから家で作った干物を送るって連絡あったんだよね。鯵かなんかだと思うんだけど、みんな貰ってくれない？俺、あんまり自炊しないのにいっつも送ってくるんだよね。」

佳乃「亮のお母さんは食生活を心配してくれてるんだよ。でも食べきれない分はもらいたいな。」

春菜「私も欲しい！私、お魚大好き。」

亮「オッケー。じゃあ届いたら二人には連絡するよ！」

佳乃「じゃあ、そろそろ終わりにしようか？ レポートやらなきゃ。」

春菜「そういえば情報科学のレポート、先生からメールきてるんだよね？メールメールっと。」

亮の着信音がなりSMSが届く。
亮（独り言）「あれ？　もう干物が届いたのか？　ずっと家にはいたはずだけど・・・」
亮「みんな、もうすぐ干物が届くかも。不在通知来たから、再配達依頼しとくね。」

亮がリンクをクリックすると宅配業者風の画面。ポップアップ表示がありOrange IDの入力が促される。面倒に思いながらも促されるまま入力をしていく亮。

一方でメールを探していた春菜、急に驚いた表情。
春菜「あれ、何！？Amasanからメールがきてる・・・
「アカウントが停止されました」ってどういうこと？昨日注文した分がどうかしたのかなぁ！？」

佳乃、不審に思う
佳乃「春奈、それどんなメール？」

春菜、画面を眺める。
春奈「Amasanからのメールには見えるけど...」

亮、次の画面で追加のコードを要求される。
亮「あーもう、なんか面倒なことになってきた！」

佳乃「亮はどうしたの？」

亮「再配達を頼みたいだけなのに、OSが古いとか確認コードがどうとかで..」

佳乃「なんで再配達でOSが古いとか言われるんだろ… ちょっと亮、最初に届いた不在通知みせてくれない？」

亮、最初のSMSをスクショしてLIMEで送信する。
亮「えーと、これだけど。」

佳乃「これって・・・二人ともまずは落ち着いて、うっかりIDとかパスワードとか入力しちゃだめだからね。」

春菜「やっぱり？」

亮「え！？　何が？　俺、もうパスワード送っちゃったよ。」

亮「え！？　どういうこと！？　お魚、ひもの、鯵あげるんだから教えて？」

【解説編】

■それぞれの部屋

天の声「亮君、うっかりIDとパスワードを入力してしまいましたね。それは恐らく偽のサイトと考えられます。今ならまだ間に合うかもしれませんので、すぐに入力したパスワードを変更しましょう。」

慌てながら
亮「はい、今すぐやってみます！」

天の声「まずは公式サイトに行って、サインインするところから始めてください。」

亮「な、なるほど…」

天の声「実在する企業などを騙ったメールやショートメッセージを送信して、偽のウェブサイトへ誘導し個人情報をだまし取る行為は「フィッシング」と呼ばれます。特に電話番号で送信できるショートメッセージを使ったものは「スミッシング」と呼ばれています。
これらのフィッシングでは、メッセージの受信者を偽のWebサイトに誘導し、アカウント情報などを入力させて、情報を盗み取っていきます。
現在では、宅配業者やオンラインショッピング、クレジットカード会社、銀行などを騙るメッセージが多く確認されています。これらの詐欺メッセージは手あたり次第に日々大量に送られているため、うっかり引っかかってしまうことがあるかもしれません。」

春菜「私も、普段は無視しているのですが、ちょうど買い物をしたすぐ後だったので、慌ててしまいました。」

佳乃「亮もタイミングが悪かったよね。」

天の声「過去にも、学生や教職員に対して、情報センターを騙って偽のWebサイトに誘導し、アカウント情報を不正に入手するといった詐欺行為も確認されています。」

春奈「情報センターを騙るメールとか、うっかり信じてしまいそう・・・今回、私に来たメールも、見た目はいつもと変わらないし、差出人もそれっぽい感じでした。」

佳乃「亮が受け取ったショートメッセージのURLは、宅配業者っぽかったけど偽物だと思いました。」

天の声「そうですね。どんなに巧妙に作られたメッセージでも、Webアドレスの偽装はできません。偽のサイトでは普段使っているサイトとはWebアドレスが異なっていますので、まずはそこで見分けることができます。」

佳乃「実際の被害も多いのですか？」

天の声「乗っ取られたアカウントに紐付いていたクレジットカードが使われてしまい、ものの数十分で限度額まで買い物されてしまったという例も報告されています。

クレジットカードを利用していない場合でも、今回の亮君のようにスマートフォンで使うアカウントが乗っ取られてしまうと、そのスマートフォンから乗っ取られたアカウント情報を切り離すことすらできなくなってしまいます。こうなると、そのスマートフォンを初期化して新しいアカウントで使い始めることすらできなくなります。アカウントが乗っ取られることの代償はとても大きなものになるのです。」

春菜「とても怖いですね。何か対策はできますか？」

天の声「メールやショートメッセージに記載されているリンクについては、クリックする前に信頼できるサイトであるかどうかを確認する、といった習慣をつけておくことが重要です。日ごろから注意深く観察する習慣ができていれば、タイミングよくフィッシングに遭遇したとしても簡単には騙されないでしょう。
よく使うサイトはブックマークする、ブラウザのパスワード自動入力機能を使う、公式アプリを使うといった方法も有効です。大手宅配業者ではSMSを連絡手段として使っていない、ということも覚えておきましょう。」

亮「やった！パスワード変更できたぞ！もしかしたらぎりぎり間に合ったのかも。」

天の声「それはよかったですね。確認コードを送っていなかったので被害を食い止めることができたのかもしれません。」

春奈「もし被害を受けてしまったらどう対処すればいいですか？」

天の声「その場合はアカウントの発行元などのサービス提供者、警察、国民生活センターなどに相談する必要があります。とにかく素早い対応が肝心ですので、おかしいと気づいたらすぐに行動を開始してください。」

一同「分かりました！！」