手話定期便　R4　４月　「偽メールにご用心！」

あなたは、自分は詐欺にはだまされない、という自信がありますか？
私も自信があったんです。でも…　私の経験をお話しします。

先日、いつも利用している大手通販サイトからパソコンにメールがきました。
そこにはこんなことが書かれていました。
会社のロゴも、画面の色も、いつものその会社のメールと同じなので、「それは大変！急いで更新しなければ」と、慌ててクリックしようとしました。
でも、よーく見ると、メールやサイトのアドレスがいつもとちょっと違うし、クレジットカードにはまだ有効期限があるはず。おかしいと思い、公式サイトで確認すると、そんなお知らせはありませんでした。調べてみると、それは偽サイトに導くための偽メールでした。
偽メールは、ロゴや色なども本物に巧妙に似せてあり、ちょっと見ただけでは区別がつきませんでした。しかも、警告などの文字でこちらを焦らせて、冷静な判断ができなくさせます。危ないところでした。

これは「フィッシング詐欺」といい、電話を使った「オレオレ詐欺」などとともに増えています。フィッシング詐欺は、実在する企業を装ってメールやＳＭＳを送って、偽のサイトに誘導し、そのサイトでＩＤ・パスワードやクレジットカード番号といった情報を入力させて、入手したＩＤ・パスワードなどを使って、お金や商品をだまし取ります。
よくあるのが、スマホの SMS で、実在の社名を語り、宅配の荷物を預かっているとか、携帯料金が未納、などの文の後に、偽物のサイトのアドレスが載っているもの。

今紹介したメールは、実際に私のところに来たものです。他にも有名な企業名でメールが届きます。
こんなメールが来ても、
①絶対にアクセスしないで、周囲や専門機関に相談して！
②アクセスしてしまっても、ID・パスワード、クレジットカードなどの情報を入力しないで！
③もし、ID などの情報を入力してしまった場合は、こちらへメールでご相談ください。
　長野県警察　サイバー犯罪に関するメール相談受付

また、すぐにクレジットカード会社などに連絡して、犯人がカードを悪用できなくすることも大事です。

詳しくはこちらをご覧ください。
　フィッシングに注意／長野県警察

犯人はあなたをだまそうと狙っています。くれぐれもご注意を！

長野県警察
サイバー犯罪に関するメール相談受付
https://s-kantan.jp/pref-nagano-u/profile/userLogin_initDisplay.action?nextURL=CqTLFdO4voandR8QPP6UhzQ9f2VYJzSn7Hr%2FNHcoupZFoc0JHHL13yArYaGWSZj5aSxl26Fva8fj%0D%0Al7fQcrqDs4EXzqYf08jE%2F6pHiGwGKPc%3Djmckfl2ED%2FM%3D%0D%0A

フィッシングに注意
https://www.pref.nagano.lg.jp/police/anshin/cyber/boushi/fishing2.html