

你会成为网络诈骗的受害者吗？ Could you be a victim of online fraud?

Hello. This is 6 Minute English from BBC Learning English. I'm Neil.

大家好。这里是 BBC 学习英语栏目的六分钟英语。我是内尔。

And I'm Georgina.

我是乔治娜。

Are you good at remembering your computer passwords, Georgina?

你擅长记你的电脑密码吗，乔治娜？

Um, not really, Neil—I mostly use something easy to remember, like my mother's maiden name or the street where I was born.

呃，不是很擅长，内尔——我基本上会用一些容易记的东西，例如我妈妈的娘家姓或我出生的街道。

Or the name of your first pet!

或者是你的第一只宠物的名字！

Yes, me too—but we should be more careful about online security, Georgina, because of a worrying trend, and the topic of this programme—online fraud.

是的，我也是——但是我们应该注意网络安全，乔治娜，因为最近一股令人担忧的趋势，也是本期节目的话题——网络诈骗。

Online fraud involves using the internet to trick someone into giving away their money or data.

网络诈骗包括使用互联网来骗取某人的钱或数据。

It takes many forms, from deceptive emails which trick us into paying money to the wrong bank account, to the theft of credit card details.

它有很多形式，从诱骗我们给错误的银行账号转账的欺骗性电子邮件到盗取信用卡详情。

It's regarded by some as a highly profitable and relatively low-risk crime, so in this programme we'll be finding out why it's so easy for criminals, or fraudsters, to steal our money.

它被某些人看作是高利润且相对低风险的犯罪，所以在本期节目中，我们要探究为什么偷取我们的钱财对于犯罪者或诈骗者来说这么容易。

And of course, we'll be learning some related vocabulary along the way.

当然我们也会学习一些相关词汇。

But first, it's time for our quiz question.

但是首先是我们的问题。

In July 2020, nine British men were arrested for defrauding the Coronavirus Job Retention **Scheme**—a government fund for workers who've lost their job to Covid-19. They set up fake companies and applied fraudulently for money.

添加的词汇

scheme

英:/ski:m/ 美:/ski:m/

n. 计划；组合；体制；诡计 vi. 搞阴谋；拟订计划



扫码APP内查看
每日英语听力

在2020年七月，九个英国男性因为骗取新冠工资补助计划——政府转为因为新冠而失业的工人而设的资金——而被捕。他们成立了假公司并申请补助来骗取钱财。

But how much money has been claimed in total through the coronavirus job **scheme** in the UK?

但是英国的新冠工资补助计划一共支付了多少钱呢？

Is it a) 17 billion pounds, b) 27 billion pounds, or c) 37 billion pounds?

是 A. 170亿英镑，B.270亿英镑，还是 C. 370亿英镑？

Hmm, it must be a lot, so I'll say a) 17 billion pounds.

嗯，肯定是很多钱，所以我要选 A. 170亿英镑。

OK, Georgina, we'll find out later.

好的，乔治娜，我们稍后会揭晓答案。

Now, Rachel Tobac, CEO of Social Proof Security, is an expert in cyber crime.

Social Proof Security 公司的 CEO 瑞秋·托巴克是一位网络犯罪方面的专家。

She describes herself as an "ethical fraudster".

她把自己描述为一个“有道德的诈骗犯”。

Businesses wanting to combat fraud employ her to hack into their computer systems to find their weak spots.

想要对抗诈骗的行业聘请她黑进他们的电脑系统来找到他们的弱点。

Here, Rachel explains to BBC World Service programme, The Inquiry, how getting people's information is the key to online fraud.

瑞秋向 BBC 世界服务节目《询问》解释为什么获取人们的信息是网络诈骗的关键。

The reason why we're able to do that, from an attacker mindset, is because we use what's called OSINT-open source intelligence.

从一个攻击者的思维模式来看，他们能够那样做的原因是因为我们使用了一个叫做 OSINT——开源情报的东西。

We look up everything about you.

我们查看有关你的一切信息。

We can figure out who your assistant is, who your accountant is on LinkedIn.

我们可以在领英上弄清楚你的助手是谁，你的会计师是谁。

We know what emails you use from screen shots that you've put on your Instagram.

我们通过你上传到 INS 上的截屏知道你的电子邮件。

Rachel looks at fraud from a criminal's mindset-someone's way of thinking and the general attitudes and opinions they have about something.

瑞秋从一个犯罪者的思维模式——某个人的思考方式以及他对一些事物的态度和观点——看待诈骗。

From a fraudster's perspective, the most valuable thing is intelligence-secret information about a government or country, or in this case a person, such as the information people unwittingly post on social media.

从一个诈骗犯的视角来看，最有价值的东西就是情报——某个政府或国家的机密信息，或者在这里指的是个人信息，例如糊里糊涂发布在社交媒体上的信息。

Fraudsters use this intelligence to build up a picture of someone's online activity.

诈骗犯利用这个情报来建立某个人的在线活动图景。

And as BBC World Service The Inquiry presenter, Charmaine Cozier, explains, there are many ways of doing this.

但是如 BBC 世界服务节目《询问》的主持人查曼茵·克孜尔解释，做到这一点的方式有很多。

Fraudsters have thousands of cover stories but the end goal is always the same—to trick people out of cash or possessions.

诈骗犯有千变万化的伪装，但是最终的目的始终不变——骗取人们的现金或财产。

Rachel says they have options for how to do that.

瑞秋说他们有不同的方法能够达成目的。

Login details stolen during a data breach from one company, often using software or viruses called malware, are used to infiltrate customer accounts at another.

在公司出现数据泄露时偷取的登录详细信息，通常是使用叫做恶意软件的软件或病毒，被用来潜入另一个客户的账户。

To access people's data, fraudsters use cover stories—false stories told in order to hide the truth.

要获取人们的信息，诈骗者们会使用捏造的故事——为了掩藏真相而说的假故事。

For example, they may pretend to be calling from your bank or credit card company.

比如，他们可能会假装成来自于你的银行或信用卡公司的电话。

If people believe these cover stories and share personal data, this can result in a data breach—an occasion when private information can be seen by people who should not be able to see it.

如果人们相信了这些捏造的故事，并且分享了个人信息，这可能会导致数据泄露——个人信息会被不应该看的人看到的情况。

Malware—computer software and viruses that are designed to damage the way a computer works—can also be used to gain login details and passwords...

恶意软件——被设计用来破坏电脑工作方式的电脑软件和病毒——也可以用来获取登录详细信息和密码.....

...data which is then used to infiltrate other online accounts—secretly enter a place, group or organisation in order to spy on it or influence it.

.....之后会被用来潜入——为了窥探或造成影响而偷偷地进入某个地方、团体或组织——另一个网络账户的数据。

Modern fraudsters are so devious at collecting online information that many victims only realise what's happened after their bank accounts have been emptied.

现代的诈骗者们收集网络信息的方式过于迂回，以至于很多受害者直到他们的银行账户被掏空才意识到发生了什么。

Which I guess was the mindset behind those British fraudsters you mentioned earlier, Neil.

我想这就是你刚刚提到的英国诈骗者背后的思维模式，内尔。

Ah, yes, the nine men who tried to defraud the Coronavirus Jobs Retention ***Scheme***.

啊，是的，那九个试图诈骗新冠工资补助计划的男性。

Remember for my quiz question I asked you how much the ***scheme*** has paid out in total so far in the UK.

记得我在问题中问你这个计划目前在英国总计支付了多少钱。

I said, a) 17 billion pounds.

我说的是 A. 170亿英镑。

Well, in fact it's even more—the correct answer is b) 27 billion pounds.

嗯，事实上更多——正确答案是 B. 270亿英镑。

Luckily, the 495 thousand pounds which these fraudsters tried to steal was recovered.

幸运的是，这些诈骗者试图窃取的49.5万英镑已经被找回。

Even so, Neil, I think I'm going to change my passwords soon!

即使这样，内尔，我想我要马上去更改我的密码！

Better safe than sorry!

安全总比遗憾好！

Good idea, Georgina.

好主意，乔治娜。

In this programme, we've been hearing about the rise in online fraud, often committed when fraudsters gain intelligence-secret information about a person posted on the internet.

在本期节目中，我们一直在听有关于网络诈骗兴起的内容，这些诈骗通常是在诈骗者获取了情报——发布在网上的某个人的机密信息——时发生的。

These criminals' mindset, or mentality, is to surreptitiously find information by creating a cover story—a false story someone tells in order to hide the truth.

这些罪犯的思维模式，或者说心理，是通过捏造故事——某个人为了掩盖真相而说的假故事——偷偷地找到信息。

By posing as clerks from your bank, for example, they might be able to access sensitive private information which they should not be able to see—an event sometimes called a data breach.

例如，通过冒充你银行的员工，他们可能会获取他们不该看到的敏感的个人信息——这种情况有时叫做数据泄露。

Another way fraudsters infiltrate—or gain access secretly, without permission—is with the use of malware—computer software and viruses designed to damage the way a computer works.

诈骗者潜入——或者说在没有允许的情况下悄悄进入的另一种方式是使用恶意软件——被设计用来破坏电脑工作方式的电脑软件和病毒。

If you want to find out more about keeping yourself safe from online fraud, search the BBC website using the term, 'cyber security'.

如果你想要了解更多保护自己不受网络诈骗的内容，请是用关键词“网络安全”搜索 BBC 的网站。

And if you like topical discussion and want to learn how to use the vocabulary found in headlines, why not check out our News Review podcast?

如果你喜欢话题讨论并且想要学习如何使用标题中的单词，何不查看我们的新闻评论播客呢？

We also have a free app you can download for Android and iOS.

我们还有一个在安卓和 iOS 平台上使用的免费下载的 APP。

And for more trending topics and real-life vocabulary, look no further than 6 Minute English, from BBC Learning English.

要获得更多话题和真实生活中的词汇，请继续关注 BBC 学习英语栏目的六分钟英语。

See you next time. Bye!

下次见！

Goodbye!

再见！
