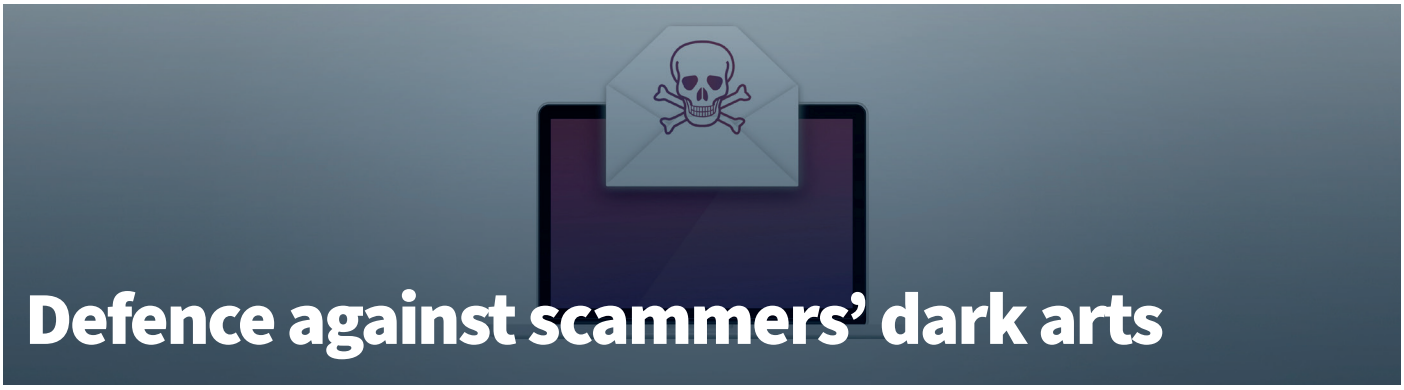
RAYMOND JAMES



Defence against scammers' dark arts

Stay sceptical – and a step ahead – of scammers

Any time there is trouble in the world, like a natural disaster or global pandemic, you can expect fraud artists to emerge like worms after a rainstorm. Scammers read headlines, too. Posing as an NHS employee, charity fundraisers, bank representatives and government agents, scammers will use any angle to get people to hand over hard-earned assets. Coronavirus-related scams had cost Britons more than £11 million by 8 July, according to the National Fraud and Cyber Crime Reporting Centre.

The good news is that most threats are easily thwarted with a good defence. Remember, it's unlikely the scammers are specifically targeting you (although it doesn't always feel that way); they cast a wide net looking for low-hanging fruit. A healthy dose of scepticism combined with easy-to-implement security measures can put you back in the driver's seat.

Scammers exploit highly stressful moments by injecting even more emotion, both positive and negative. Over the phone, they'll threaten arrest, warn of lost opportunity or take the role of the earnest good guy just trying to save you future headaches by acting now.

Many of the most common scams are old as the hills; however, some emerging tactics may be surprising, especially now that information is so publicly accessible online. The case studies below are based on real-life scams reported by government authorities and information security experts.

Appearances can be deceiving while caller ID seems like simple, reliable technology, there is no guarantee that what shows up on your phone is accurate. "Caller ID spoofing" can make it seem like you are getting a call from any number, regardless of where it originated.

Chelsea was initially sceptical when her credit card company called to inform her of a problem, but the service representative knew her name, date of birth, address and even her three most recent purchases. Since everything seemed to check out, Chelsea cleared up the supposed issue and went on her way.

But a nagging feeling remained. She called back and learned that "she" had apparently ordered a refund for a substantial over-payment. Luckily, the card issuer's policy was to mail a check, rather than deposit it in another account, but Chelsea made sure to keep an eye on the mailbox until it arrived.

Unbeknownst to Chelsea and the card issuer's representatives, criminals had spoofed the phone number of the card issuer when calling Chelsea, and the scammers had spoofed Chelsea's number when calling the card issuer. And because of lax data security at the card issuer, the scammers were able to find out Chelsea's last three transactions with just the telephone number as confirmation, giving the scammers credibility when they spoke to her, but not access to her entire account.

So, as the actual card issuer representative asked questions to the scammers to establish their identity as "Chelsea" to access the full account, real Chelsea was providing those answers to the scammers, allowing them to complete the impersonation and order a refund.

SCAM DEFENCE

Hang up. Call back using the number on the company's website or the back of your card to ask questions and verify the previously stated issue or account hold. At the cost of a little hold music, you can resume your business if the call was legitimate.

> Scammers defraud an estimated £190 billion each year according to the 2017 Annual Fraud Indicator, a number that has likely risen since then

Be aware that information you believe is confidential may actually be available online, including information you post on your own social media. Financial data leaks, breaches and security failures have become all too common. Know what could be out there and defend your information with unique passwords for each account. There may also be more information about you in your council voting registration, parking or speeding tickets and other open government sources that you wouldn't suspect.

Enable multifactor authentication on all accounts but especially for your network provider, bank accounts, email and other important accounts.

ONE LITTLE NUMBER

Bill was selling antique chairs online when he got a text expressing interest. After a brief negotiation over price, the person texted that they wanted to verify Bill was a legitimate seller, you know, for security reasons. He was told he would receive a six-digit confirmation number and to repeat it to the potential buyer.

Moments later, he received a text message containing six digits from an unknown number. As a savvy seller, he immediately stopped responding to this "buyer," knowing that had he given up the digits, he would have given away the keys to his electronic identity.

While the scammers were texting him, they were also hitting the "forgot my password" button on one of his online accounts, likely his email account, which is a common starting point for scammers. With that number, they would have been able to change his password and the telephone number associated with his account.

From there, the scammer would have quickly commandeered his email account and gotten access to his many online service accounts, repeating the "forgot my password" trick then using the hijacked email to verify identity and use that information to access his finances.

SCAM DEFENCE

Think critically when asked for personal information. Does the request make sense? Can it be verified independently? There is no reason to text a verification number you received by text. Instead, your login actions should generate two-factor verification numbers required to access a website or account.

Keep your phone locked with a PIN or other security measure. A stolen phone can be used to hijack many of your online accounts.

Secure existing accounts and consider creating an email address to use while buying or selling online to thwart low-effort scamming attempts.

Again, enable multifactor authentication on your essential accounts.

OUTSMART THEM

It may seem like the Wild West out there, but you've got the tools to put up a worthy defence and stay ahead of scheming, digital criminals. And you're not on your own. Reputable companies take cyberthreats seriously and institute multiple layers of protection in an effort to thwart relentless hackers and protect your information.

Defence against cybercrime

Create strong, unique passwords for each account. Consider using a password manager, a program or phone app that creates complex passwords for your online accounts. A single master password (which should be the strongest), known only to you, controls access to your many online accounts without you having to remember dozens.

Multifactor authentication, which requires a username and password as well as a security key usually texted to your phone, is a strong defence against compromised information.

Be wary of "mother's maiden name" type security questions as well as passwords that contain personal information. Biographical information can be easily mined through social media, news archives or public records. Try to use information known only to you.

Financial account monitoring that continually checks for signs of intrusion is available from a number of providers.

Credit freezes can be an important tool to prevent identity thieves taking on debt in your name or running credit reports for fraudulent purposes.