HSBC Private Banking

Wealth Matters - October 2019 Video transcript

Tammy Archer

Hi I'm Tammy Archer and I'm the chief information security officer for the global private bank at HSBC. And I'm very passionate about helping our clients to stay safe online.

So as a high net worth client, you need to be on the lookout for phishing emails. Phishing emails are sent by hackers or fraudsters, and they contain a link in an email that might look real, but the link doesn't lead where it says it's going to go. Instead it has malware, hidden within it, that then gets downloaded to your hard drive or your laptop or your mobile device.

This software can either be used to steal your information from your device or it can be used to encrypt your hard drive as part of a ransom attack.

Vishing is where a criminal or a hacker will phone you up and will ask you for information, usually your password.

If you ever receive a phone call from anybody asking for your password, this is highly unlikely that it is going to be legitimate. Do not ever give your password to anybody over the phone. If you feel that there's a legitimate reason for you to give this information or you need someone to act on your behalf, then ensure that it's you that is making the phone call. So hang up the phone and recall the service that you require or the person that you need to make that deal for you.

Smishing is an attack to your phone. It's where you are sent an SMS message with a link in that has malware included. Never click on a link in a text message. If your friend sends you a picture in a link in a text message, just text them back and say can you send me that link in an email please? Opening a link in an email is much safer than it is in a text message on a phone.

You may find at some point that you've either clicked a link or you've downloaded some malware from the internet when you've gone to a website, and all of a sudden, your laptop or your data starts to encrypt. This is called ransomware. If you get ransomware, you will quite often be sent an email or there will be a message as part of that attack that pops up on your screen that tells you that you need to pay bitcoin to get your data unlocked. You can either choose to pay the ransom, or if you've been prepared for a ransomware attack, you may have decided to back up your data and have a standalone copy of that data. Therefore, it doesn't matter if you get ransomware, you can rebuild all your data from scratch.

Be careful what information you expose about yourselves, your families or your business online. This information, if it's sensitive, can be used to extort information out of you. If you don't encrypt and store this information, both at rest on your hard desk or in transit across the internet using a VPN, this information can be intercepted and used against you.

A good rule of thumb is never send any information about yourself, your business across the internet that you wouldn't like to see across the front page of the Sunday paper.

Another threat is a man in the middle attack. A man in the middle attack happens when we're out and about at a hotel, a coffee shop or even at an airport, where we accidentally join a rogue wifi service. A rogue wifi service may look like a legitimate service, but they're more often than not a free wifi. This means that there's no password to join to the service. You may even get a warning to say this service might not be secure. I would recommend that you use your own personal wifi.

If you'd like any further advice about anything that I've mentioned today, speak to your relationship manager.