Lesson 5: Cybercrime & scams

Here are some names and descriptions onyber Scams how online criminals try to take your money. Read the description ofeach scam, and then decide which name gees with each text. Click on the nanzefirst and then select the space in the text which goes with the name. Keep going until you have matched them all.

[.... A person selling a product on the internet receives an email from someone (generally abroad) who offers to buy the product. For some reason, the buyer overpays. Perhaps because he says a friend owes him money, and the friend will send the money to the seller. The seller should take What he is owed and pass on the rest to the buyer. The money always arrives as a beautifully forged banker‘s draft. This is a sort of cheque written by the bank, and was once considered almost as good as money. Once the draft has been paid in, the bank will often show that the money is in the sellers account. So the seller sends off the extra money which was 'overpaid' and often the thing he is selling as well. Only later does his bank discoverthe forgery and take back its money. This means that the seller has not only lost what he was selling, but some extra cash as well.

user receives an email telling him that there is a problem with his bank account, or that because new security software has been installed, he must re-enter his account details. A link is given in the email that leads to Van officialalooking web page. In reality, the web page is run by a scammer who takes the security information given and immediately uses it to withdraw money from

his Victim’s account. Phishing emails can be detected by looking at the message code (which often shows that it was sent to many people at one time) and by looking at the link, which often goes to a different site to the one which which it shows in the email. It is easier to see these things if you do not View your emails in HTML. Look for other signs such as the message starting ’Dear customer‘ instead of using your name . If in doubt close the email and type the address of your bank into the URL banpf a newly opened browser window instead. This might be an .mp3 of your favourite song, it might be a spam email offering you a $300 software package for $3 the one thing you can be sure of is that the person who produced the original product is not going to see any of the money. Sometimes, you get exactly what you have pain for congratulation; you have found an honest thief. Sometimes you get a bit more than you pain for some bonus software which

l .... You get an email from someone who says that he heard of you through a 'business acquaintance' (though the email does not give the name). The writer of the email is usually from Africa, or from Asia, and has suddenly found himself in charge of a massive fortune. Sometimes the writer pretends to be the relative of a dead afiican politician, ' or the manager of a bank, or even someone dying of a horrible disease who wants to give her money away to a deserving cause. Whatever happens, the writer wants you to supply your personal details and the number of your bank

account so that countless millions of pounds can be deposited there. Except= it turns out that there is a small processing fee, and that another official needs to be bribed, and so the steady requests for money go on, each promising that this is the last before the big payout. Finally you may be asked to go to the country to finalize the details which is a way of asking you to kidnap yourself and hand yourself over to some rather Scary criminals.

[.... The advertisement looks promising. 'We are an business in Latvia/Estonia/ some place far away. We need a client in your country to act as our agent. Reasonable wages for a small amount of money.' What the person answering the advertisment discovers is that the company wants them to take payments from people in their country, put them together into a single payment, and send this abroad. lt sounds reasonable, until you realize that one of the biggest problems for people running phishing scams is that banks are suspicious of cash transfers abroad, and often check with the holders of the account that this is what they wish to do. So the cyber mule takes the money stolen from accounts by phishing and transfers it to the criminals abroad once or twice. lt does not take long before the police have caught up with him and his bank account has been seized, but by then the real Criminals have found another victim.

Lección 5: Ciberdelincuencia y estafas

Aquí hay algunos nombres y descripciones sobre estafas de cómo los delincuentes en línea intentan tomar su dinero. Lea la descripción de cada estafa y luego decida qué nombre tiene cada texto. Primero haga clic en el nanze y luego seleccione el espacio en el texto que va con el nombre. Continúa hasta que los hayas emparejado todos.

[.... Una persona que vende un producto en Internet
recibe un correo electrónico de alguien (generalmente en el extranjero) que
ofertas para comprar el producto Por alguna razón, el comprador
paga excesivo Tal vez porque dice que un amigo le debe
dinero, y el amigo enviará el dinero al vendedor.
El vendedor debe tomar Lo que se le debe y pasar el
descansar al comprador. El dinero siempre llega como un
bosquejo del banquero bellamente forjado. Este es un tipo de cheque
escrito por el banco, y una vez fue considerado casi como
bien como el dinero Una vez que se pagó el giro, el
el banco a menudo mostrará que el dinero está en los vendedores
cuenta. Entonces el vendedor envía el dinero extra que
fue 'pagado en exceso' y a menudo también lo que está vendiendo.
Solo después, su banco descubre la falsificación y toma
respalda su dinero. Esto significa que el vendedor no solo ha
perdió lo que estaba vendiendo, pero algo de efectivo extra también.
el usuario recibe un correo electrónico diciéndole que hay
un problema con su cuenta bancaria, o eso porque
software de seguridad ha sido instalado, debe volver a ingresar a su
detalles de la cuenta. Se proporciona un enlace en el correo electrónico que conduce a
Sitio web de Van ofiaialooking. En realidad, la página web es
dirigido por un estafador que toma la información de seguridad
dado e inmediatamente lo usa para retirar dinero de

la cuenta de su Víctima. Los correos electrónicos de phishing pueden ser detectados por
mirando el código del mensaje (que a menudo muestra que
fue enviado a muchas personas a la vez) y al mirar
el enlace, que a menudo va a un sitio diferente al que está
lo cual se muestra en el correo electrónico. Es más fácil ver
estas cosas si no ve sus correos electrónicos en HTML.
Busque otros signos, como el mensaje que comience 'Querido
cliente 'en lugar de usar su nombre. Si tiene dudas cierre
el correo electrónico y escriba la dirección de su banco en el
URL banpf una ventana del navegador recién abierta en su lugar.
Esto podría ser un .mp3 de tu canción favorita,
podría ser un correo electrónico no deseado que le ofrece un software de $ 300
paquete por $ 3 lo único de lo que puede estar seguro es que
la persona que produjo el producto original no es
ir a ver el dinero. A veces, obtienes
exactamente lo que tienes dolor para felicitarte; tú
he encontrado un ladrón honesto. A veces obtienes un poco
más de lo que le duele a algún software de bonificación que

Yo recibo un correo electrónico de alguien que dice que él
oído de ti a través de un "conocido de negocios" (aunque el
el correo electrónico no da el nombre). El escritor del correo electrónico es
generalmente de África, o de Asia, y de repente ha encontrado
él mismo a cargo de una gran fortuna. A veces el
el escritor pretende ser el pariente de un político a fi cial muerto '.
o el gerente de un banco, o incluso alguien que muere de un
horrible enfermedad que quiere darle dinero a un
causa meritoria Pase lo que pase, el escritor quiere que
proporcione sus datos personales y el número de su banco

cuenta de modo que incontables millones de libras pueden ser
depositado allí. Excepto = resulta que hay un pequeño
tarifa de procesamiento, y que otro funcionario debe ser sobornado,
y así siguen las constantes solicitudes de dinero, cada una prometedora
que este es el último antes del gran pago. Finalmente puedes ser
pidió ir al país para finalizar los detalles, que es una
manera de pedirte que te raptes y te entregues
para algunos criminales más bien Scary.

[.... El anuncio parece prometedor. 'Somos un
negocios en Letonia / Estonia / algún lugar lejano. Necesitamos una
cliente en su país para actuar como nuestro agente. Salarios razonables
por una pequeña cantidad de dinero. Lo que la persona contesta
el anuncio descubre que la empresa los quiere
para recibir pagos de personas en su país, póngalos
juntos en un solo pago, y enviar esto al extranjero. lt
suena razonable, hasta que te das cuenta de que uno de los mayores
problemas para las personas que ejecutan fraudes de phishing es que los bancos
desconfían de las transferencias de dinero en efectivo en el extranjero, y a menudo verifican con
los titulares de la cuenta que esto es lo que desean hacer.
Entonces, la mula cibernética toma el dinero robado de cuentas
phishing y lo transfiere a los delincuentes en el extranjero una vez o
dos veces. No pasa mucho tiempo antes de que la policía se haya puesto al día
con él y su cuenta bancaria ha sido confiscada, pero para entonces
los verdaderos criminales han encontrado otra víctima.