



## Banking and phishing scams

### The set-up

You receive an email, asking you to update your account details.

### The hook

It looks genuine. You type in your PIN number and password.

### The sting

You have just given scammers access to your money and your financial identity. They will take both.

## What a banking or phishing scam looks like

You receive an email from what appears to be a bank or financial institution, giving some reason why you need to confirm your account details into a return email or website. A false Internet Banking log on page could appear (which is a replica of an existing legitimate business and site) and account information may be captured if details are entered. These details are then used to steal your money.

### What's phishing?

Phishing - also called 'carding' or 'brand spoofing' - is fishing by some method (like down the phone line or by email) trying to get your bank account numbers, passwords and credit card numbers.

These emails often ask for information such as credit card numbers, bank account information and passwords that will be used to commit fraud.

These hoax emails can look genuine, using the company's logo and format, and a link which leads to a website that seems genuine, but isn't. Emails from genuine banks don't include links.

The name of the website will be similar to, but not the same as, the bank's real website. Instead of [www.bank.co.nz](http://www.bank.co.nz), the email will link to a site called something like '[www.bank.co.nz.log107.biz](http://www.bank.co.nz.log107.biz)' or '[www.scamcentral/bank.co.nz/login](http://www.scamcentral/bank.co.nz/login)'.

Most phishing emails you receive will be from scammers that say they are banks and often you are not a customer at these banks, because these emails go out in huge waves to millions of email addresses. The scammers are hoping to hit real customers of that particular bank.

They probably do not use your proper name.

There are often mistakes in spelling and grammar.

Their reasons for the email:

- upgrading security
- system maintenance
- to 'verify' your account
- to protect you from fraud
- to offer you a refund for a fee or bill.

A bank or financial institution will never ask for your password or PIN: whether by phone, email, mail or door-to-door. If someone claims to be from the bank and asks you for your password or PIN, it is a scam.

## Variations on banking and phishing scams

### Credit card scams

Scammers ask for your credit card details, because all they need to start running up bills on your account is the name on the card, the number, the expiry date and possibly the security code on the back. To get these details they may use hidden spyware on your computer; they may use phishing emails or phone calls; or they may even try card skimming to copy the information on your credit card's magnetic strip.

## Phoney fraud alert

You will be told, by phone or email, that your account has been cancelled because of criminal activity or they suspect your account details have been stolen. The bank needs your details so they can 'investigate'. They may sound authoritative, and they may even have your credit card number already. What they want is your password to unlock your account. Don't give it to them. This fraud works because banks and credit unions do sometimes contact people about suspicious activity: but they will never ask for your passwords.

## Card skimming

Scammers 'skim' your cards, copying the electronic information from their magnetic strip. Once they have your information they can 'clone' your card and access your accounts.

## Tax refund scams

You received an email claiming to offer you a tax refund. The link in the email directs you to a fake webpage with an Inland Revenue logo or a fake email address. You are asked to enter personal details, including your username and credit card details. The site is trying to use the Inland Revenue brand to try to access credit card account details of people visiting the site. Never click on any links within a suspicious email offering a tax refund, do not reply to the email, and delete it from your inbox. You should always be very careful about giving out your IRD number or your personal details. Other tax scam emails may ask you to verify your billing address and say you or someone had used your account from different locations and asks you to ring a telephone number from a landline to confirm your billing address. If someone has given their details to the people behind these sorts of tax refund scams, they should contact Inland Revenue on 0800 227 774. Suspicious emails targeting Inland Revenue customers can be reported to [phishing@ird.govt.nz](mailto:phishing@ird.govt.nz).

## Protect yourself from banking and phishing scams

- Keep your ATM and account details, PINs and passwords secret and safe.
- Check your account statements and credit card bill to make sure no-one is accessing your accounts.
- Don't share your PIN with anyone.
- Use difficult passwords that cannot be guessed.
- Don't give your account details to anyone you do not know or trust.
- Don't give out details over the phone unless you made the call and you definitely trust that the number you called is genuine.
- Don't open suspicious or unsolicited emails (known as spam). Delete them.
- Don't respond to these emails in any way. Don't reply. Never click on any links in a spam email, or open any files attached to them, or call a number included in the email.
- Never visit your bank's website by clicking on a link. It can activate all kinds of hidden programmes. Type in the website address yourself.
- Check the website address carefully. It may be similar to your bank's, or paypal's, but not quite right.
- Never enter your personal details into a website unless you are sure it is genuine.
- Never send your personal details or accounts or passwords in an email. Email is a very insecure system.
- If you receive a call, ask for a name and number so you can call them back. Check that number against a number you know to be genuine.
- If, despite everything, you think the email may be genuine, call the institution, using a number you know to be genuine. Ask their advice. Do not use the number listed in the suspicious email, unless you know it is the right one. The scammers may have used it to add to the email's false sense of legitimacy.
- Don't buy anything over the internet using your credit card details unless you know and trust the business. Ensure that if you make a payment to a trader via the internet that the payment page is secure, normally demonstrated by a padlock symbol somewhere on the page, and that the website address starts with 'https://'. The 's' stands for secure.
- Don't use software on your computer that fills in forms for you.
- Keep safe from credit card skimming. This is the type of fraud that copies the contents of your card's magnetic strip. Never let your card out of your sight at a store, say 'no' to requests to swipe your card through more than one machine, and if an ATM has a suspicious device attached to its card slot, don't use it (and report it immediately). If you think your card has been skimmed, or you notice unexpected items on your credit card statement, contact your bank immediately.
- Order a credit report every year to make sure no-one is using your name to borrow money or run up debts.

## Help protect others from phishing scams

If you have received this kind of scam letter, email, phone call or experience, please share your story. We will treat your report in the strictest confidence and remove your personal details before posting your story on our site.

[Report your scam story to us.](#)

