



major corporation – a bank, a credit card company, a telephone company. The phisher creates an email which looks like it probably came from that company and sends it to as many people as possible. The email will perhaps explain that the company is updating its customer records and needs you to confirm your details. Clicking on a link in the email will take you to the fake site where you will be asked for bank account details, passwords, credit card details, pin numbers and so on. Once the phisher has this information they have your online identity and identity theft has cost banks and credit cards issuers about \$2.4 billion in the last 12 months alone. Small fry compared to the billions lost by “traditional” credit card fraud, but it’s a growing phenomenon.

phishing
(FISH.ing)
pp. Creating a replica of an existing Web page to fool a user into submitting personal, financial, or password data.
—*adj.*
—*phisher n.*

One of the major internet security organizations reported that it intercepted 14 phishing messages in August 2003. In January 2004 it intercepted almost 340,000. Almost every English speaking continent has been subjected to phishing attacks over the last year with organizations such as Citibank, Visa, Barclays, NatWest, ANZ and Westpac (to name but a few) being targeted. While the initial impact on those companies was on their brand and reputation, it is quickly becoming a financial and legal issue too.

How do you protect yourself? Well, a large dose of common sense coupled with a measure of perpetual distrust is perhaps the best place to start. Be cautious with any site that asks for personal information such as PIN codes or passwords. Check the URL – if it looks like a Citibank web site but the URL is www.phish4tea.com, its probably not a Citibank web site. Check the details in the email – an email from your bank asking you to confirm personal details would probably include your name (spelt correctly) rather than starting “Dear Valued Client” , for example. And never, ever, ever, click on the link which says “click here to unsubscribe and never hear from us again” – all you are doing is confirming to the phisher that they’ve found a real live email account so the volume of spam (unsolicited junk mail) you will receive will go through the roof!

But don’t think it’s going to be easy – almost 60 million Americans received a phishing email last year and in one online test, almost 30% of participants couldn’t tell a phishing site from the real thing! If you think you may be part of that 30% please send me BD20 in used notes and I will tell you how to spot a scam!!

Steve Ritchie is the Chief Information Officer at Investcorp Bank in Bahrain. He has recently been elected to the Chair of the Bahrain British Business Forum.

Credit card fraud – a quick scan of your card by the waiter as he takes it to the cashpoint and within hours, someone else could be spending on your card. Sophisticated scanners and pin-point cameras at ATMs can record your credit card details and PIN and by the time you spend the money you just withdrew, a thief has cleared out the rest of your account. We’re all pretty careful about who we hand our credit cards too and about who’s looking over our shoulder when we enter our PIN number, but how much information do we freely give away without batting an eyelid?

A year or so ago, if you came across the term “phishing” you would probably assume it was a typo, but industry surveys suggest that in the last 12 months, almost half of all the “online adults” in the US had received at least one phishing email. And the rest of the English speaking world was not far behind. But hey, we’re in the Middle East, that doesn’t affect us – does it?? Indeed it does! One of the features of the Internet is that it reaches the parts that other systems fail to reach. Even though you may live in Bahrain, if you have an email account with Yahoo or Hotmail or any of the other international email providers, you will be a target for phishing. And it won’t be long before local service providers such as Batelco will feel the pressure too.

So what is phishing? Simply put, a phisher creates a web site that looks just like the web site of a