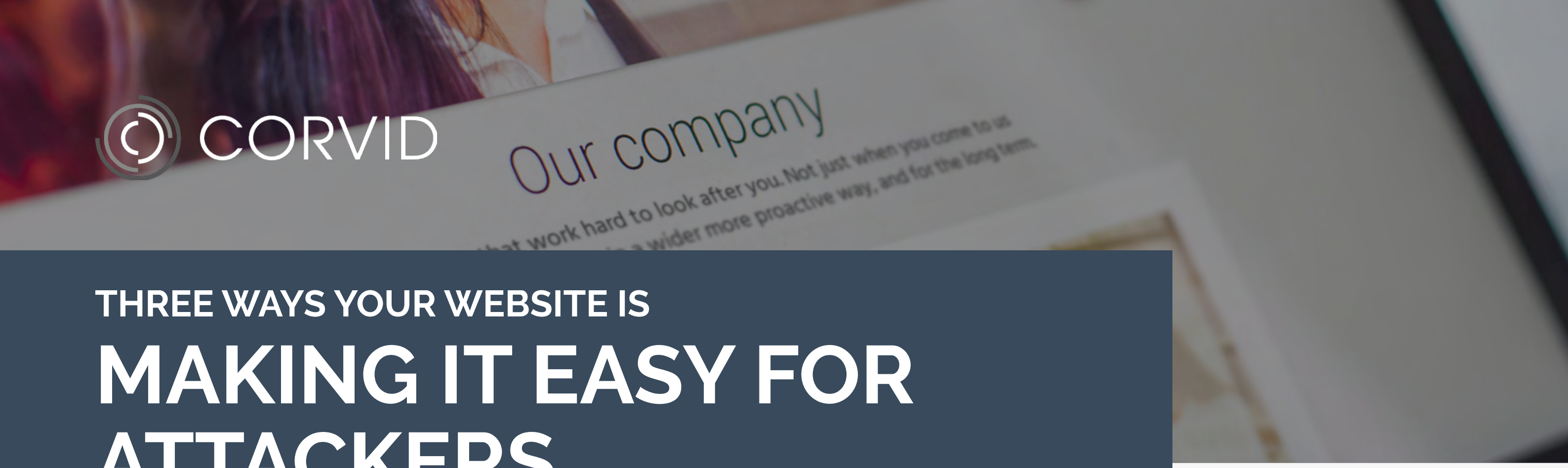


CORVID

THREE WAYS YOUR WEBSITE IS

MAKING IT EASY FOR ATTACKERS

Cyber attackers around the world are quietly appreciative of financial firms for making their job easier. With all the information they need to craft their attack laid out neatly in front of them, adversaries only need to join the dots to build the foundations of a credible impersonation attack.

Once they've spent a minute or two gathering the information they need, cyber criminals can begin socially engineering their way to the account details, assets under investment, and high profile client information you hold.

A quick internet search revealed that financial services firms have a tendency to make researching an attack a trivial task for cyber criminals. But where exactly are they going wrong?

1 Personal contact details

100% of the financial firm websites we checked listed names and email contact details for their executives and board members. No big deal, right? Surely clients want to know who they're dealing with?

An impersonation attack will only work if it convincingly impersonates an actual person. If your website is advertising the names of your staff – especially VIPs – that's the first part of the spoofed email address nailed. It will also enable cyber criminals to concoct a realistic email signature.

Corporate email accounts all follow the same pattern, so publishing contact details – even a generic 'contact@' email address – gives adversaries the consistent format of the second half of the email address. They can then spoof the domain to make it look almost identical to the genuine article. Add this to the name they've identified, and they've got a convincing email address that looks like it comes from a genuine person at your firm. Simple.

2 LinkedIn profiles and career backgrounds

100% of the sites we surveyed provided detailed career histories, and 60% provided a link to each person's LinkedIn profile.

Although sparkling credentials add credibility to the financial firm, they also give criminals personal information to work into their attack, to make it more credible and therefore more likely to succeed.

LinkedIn profiles provide the same personal insight, with the added bonus of revealing professional connections. This enables attackers to not only accurately impersonate someone at the firm, but also provide background to a relationship with the person their spoofed email is intended for. Hobbies, for example, are listed on many LinkedIn profiles, so it's not out of the question to presume a quick glance at the target's profile will give the attacker a friendly, conversational hook to their email, which implies the attacker knows them already. (As a side note, it's best not to overshare on LinkedIn either, for this very reason.)

3 Named clients

80% of the firms' websites we checked revealed their clients to the public, through a mixture of news items and named client testimonials.

It's not uncommon for businesses to shout about their successes in bagging big name clients, but it's also a terrible idea. Advertising your wealthy clients effectively paints a big target on their backs for cyber criminals. Compromising a FTSE 100 company is no easy task, but breaching their financial advisory firm is comparatively straightforward – especially if their website is generous enough to provide the information highlighted in points 1 and 2.

It's a trivial task for adversaries to check an executive's LinkedIn profile against the financial firm's list of customers to see who they're connected to. All the adversary needs to do then is use the information on the firm's website to spoof an executive's email address, and get in touch with the known customer contact, requesting funds to be diverted to alternative account details.

Anatomy of an impersonation attack

Senior Associate's contact details from the firm's website. The lowecase 'L' in the financial firm's domain name has been changed to a capital 'i'.

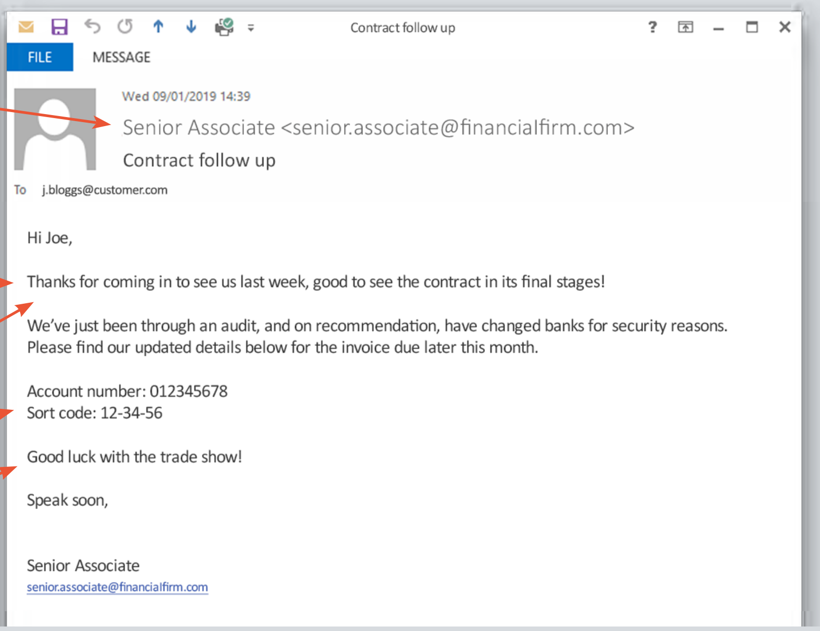
Name of client contact from Senior Associate's LinkedIn connections.

New client advertised on the firm's news feed.

Email message refers to contract finalising meeting celebrated on LinkedIn, with the client tagged in the post.

Bank details are those of the attacker.

Client advertised their attendance at an upcoming trade show on Twitter.



Wed 09/01/2019 14:39

Senior Associate <senior.associate@financialfirm.com>

Contract follow up

To j.bloggs@customer.com

Hi Joe,

Thanks for coming in to see us last week, good to see the contract in its final stages!

We've just been through an audit, and on recommendation, have changed banks for security reasons.
Please find our updated details below for the invoice due later this month.

Account number: 012345678
Sort code: 12-34-56

Good luck with the trade show!

Speak soon,

Senior Associate
senior.associate@financialfirm.com

This seemingly innocuous information sharing makes a cyber criminal's job almost too easy. Your website is the face of your business, but which mask does yours wear? Websites flooded with 'useful' contact information are prime targets for opportunistic cyber attackers, looking for a quick win. The more difficult your website makes it to spoof your financial services firm, the less likely attackers are to try their luck.

Don't make it easy for attackers

Review your website through the eyes of a cyber criminal – try to find all the components you would need to create an accurate spoof for someone at your firm. Chances are it will be easier than you think.

As well as paring down the contact information on your website, ensure your firm puts preventative measures in place to stop email attacks succeeding. PERNIX identifies spoofed email addresses and notifies users if an email isn't from the person it claims to be from, making attempted impersonation and payment diversion fraud instantly detectable. Our solution provides immediate protection, without costly or complicated setup. Want to see the difference it can make?
Get in touch with our experts to request your free 30-day trial.

CORVID