BRANDPROTECT EXECUTIVE THREAT BRIEF

brandprotect™

August 2016 | Briefing 21

THE PHISHING ATTACK IS ONLY THE BEGINNING

It has happened again. There has been a massive breach exposing emails, or credit cards or who knows what. And the press is going wild, looking for someone responsible, someone to blame. There will be stories in today's paper, and probably analysis in tomorrow's paper. But don't worry, the day after tomorrow, there will be a new breach, and the process will begin again.

Breaches are bad. Very bad. But they are the last act of a multi-stage attack process. Surprisingly, most of these major cyber events have the same evolution.

THEY ALL BEGIN WITH A PHISH.

Phishing attacks are attacks where scammers present you with legitimate looking emails, usually containing an important, time sensitive, or once in a life time offer, and try to lure you into clicking on a link to "take advantage of the offer." Phishing is the both the oldest and the newest type of attack; the simplest and the most sophisticated kind of attack.

Admit it, you've been phished, and you will be phished again. Of course you stay on your toes, vigilant, wary… **but one day, you'll relax.** That's when you will get an email that you read quickly, one you think you understand. **You'll click on the link and you'll follow the instructions you see there…**

Oops.

Phishing is much more than a personal nuisance. It is the most common way that cyber criminals begin the build-up to a major corporate breach. In fact, virtually every enterprise breach begins with a phish.

PHISHERS ARE RAISING THE STAKES.

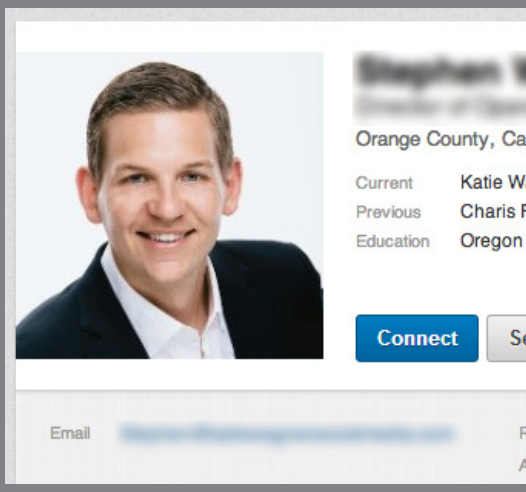
The newest generation of enterprise phishing exploits are meticulously created spoofs of official corporate emails. The scammers, using information that they gather from LinkedIn and other social networks, are able to send the email directly to you, and disguise the email so that it looks like it comes from someone you know, from the trusted corporate email domain.

These socially-engineered attacks are especially hard to detect, but they can be detected.

SOCIAL NETWORK DANGER

The modern phisher is perpetually mining social networking sites, like LinkedIn and Facebook, to gain intelligence about you, your friends, and your colleagues. They will use this information to craft ever-more convincing emails.

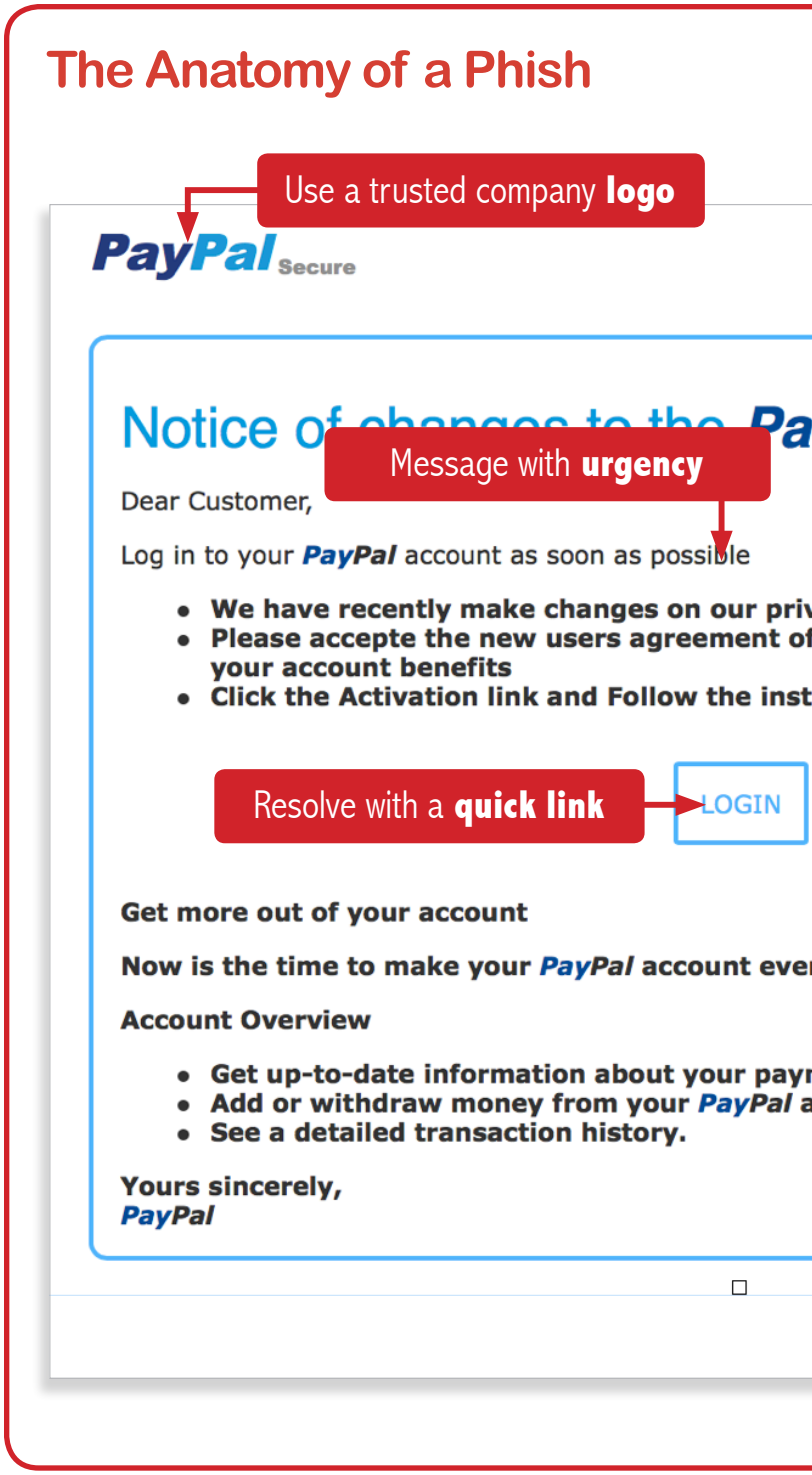
Whenever possible, try to limit the personal information that you post online or include in your profile. Take advantage of the privacy settings that are available to you to keep your profile locked down. When strangers ask to link to you, don't feel compelled to say "yes". It is better to be safe than sorry.



COMMON PHISHING TECHNIQUES

THE PLAYBOOK IS WELL KNOWN.

- **An email appearing to be from a bank, credit card company,** or other financial institution requests that you "confirm" your personal account information. Supposedly, your information has been lost, or your account is going to be closed, so it is "urgent" that you respond immediately.
- **An email from the "fraud department"** of a well-known company asks you to verify your information because they "suspect you may be a victim of identity theft."
- **An email that takes advantage of a current event**, such as a headline-grabbing data breach, which scammers used to send phishing emails with malicious links for "free credit reporting."
- **An email claiming to be from a state lottery** commission requests your banking information to deposit the "winnings" into your accounts.
- **An unexpected email from your company** asking you to verify your network credentials, or review an important document.



PROTECT YOURSELF FROM PHISHING

1. Treat any unexpected email with caution, at home or at work. **The more urgent the request, the more suspicious you should be.**

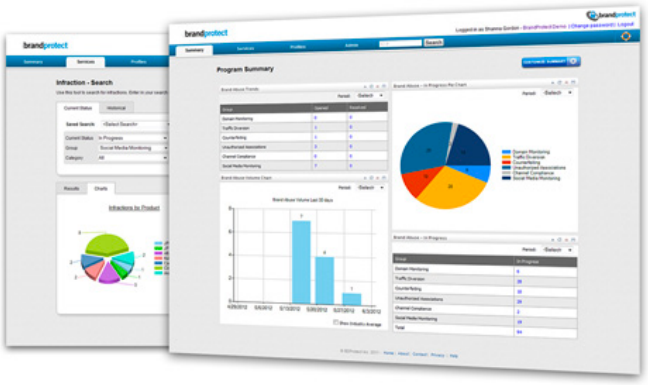
2. Legitimate organizations **will not ask you to send sensitive information via email**.

3 **Only open an email attachment if you're expecting it** and know what it contains. Be especially cautious about container files, such as .zip files, as malicious files could be packed inside.

4. Visit banking or financial websites by typing the address into the directly in the browser address bar. **Do not follow the links embedded in any unsolicited banking email**.

5. If you want to verify a suspicious email, **contact the purported sending organization directly** – but don't call the number which is provided in the email.

BRANDPROTECT ANTI-PHISHING SOLUTIONS



The BrandProtect™ SMART™ platform delivers full anti-phishing protection, through integrated domain monitoring, MX Record tracking, wide scale phish capture and evaluation, and unsurpassed mitigation services. Through the unique combination of technology based detection and initial evaluation, backed by experienced identity theft and anti-phishing specialists, the BrandProtect is able to offer detection and mitigation of generic phishing attacks, as well as the sophisticated modern phishing attacks that threaten organization with plausible, socially engineered emails. We provide enterprise-class effectiveness in each of the three major phases of anti-phishing protection. **We are constantly monitoring for new domains with names that mimic yours** and for domains with other infringing content. We have one of the industry's **most complete infrastructures for capturing phish "in the wild"**. We provide **full-scale mitigation services** to neutralize phishing attacks and phishing sites. From detection through mitigation, BrandProtect is able to provide enterprise-class anti phishing services that not only completely satisfy the needs of small and medium sized business and institutions, but also scale to meet the demands of the highest volume clients in the world.

brandprotect™

www.brandprotect.com
sales@brandprotect.com | 1.866.721.3725

For enterprises concerned about their business exposure to increasing online risk, BrandProtect™ provides a complete suite of world class Internet threat detection services to monitor the entire social Internet spectrum and mitigate business risk arising from fraudulent or unauthorized online activity. BrandProtect helps security, risk management, and marketing organizations at leading financial services institutions, large-scale retailers, insurance providers, telecoms, pharmaceuticals and more, protect their brand value and business bottom line.