DANAHER
INFORMATION SECURITY
THINK | PROTECT | SECURE | TOGETHER

Cybercrooks are getting more devious. They're targeting us with fake emails containing personalized messages designed to steal money and information.

—

You may think you're not important enough to be targeted by hackers. But you are. Even if you're not wealthy; even if your online communications only involve your friends — your personal information is of great value, and so are names of the people in your email address book and in your social networks who might respond if crooks send messages in your name.

Crooks have found it's worth taking time to learn about us individually and create targeted email messages — because we're more apt to be tricked into clicking on links — if the emails are interesting and relevant to us.

As you probably know, fake emails are called "phishing" emails. But these customized fake messages are called "spear-phishing" emails, because the crooks are "spearing" us individually.

Spear-phishing emails arrive at work and on home comupters. The messages might appear to be from Amazon, PayPal, from the IRS, from your boss, your kids' school, even from your significant-other.

This will give you an idea how sophisticated cybercriminals are becoming. First, here are some examples of spear-phishing emails that could arrive on a computer at work.

-

A woman at a large accounting firm was promoted to a management role. She posted news about her promotion on LinkedIn. Crooks were alerted to her new role, assumed she had access to the firm's important financial records, and used an online database to learn her work email address.

But they had to figure out how they could get her to open an email with infected document on her work computer. If she did, they could gain access to the accounting financial records of the firm and its clients. Here's how they did it.

The woman was active on Facebook, and her Facebook account privacy setting was set so anyone could view what she wrote. She often posted photos of her son's high school football games, which gave the crooks an idea. Visiting the high school's web page, they learned the name of the head football coach. They sent the woman an email at work that appeared to come from the coach. The email said the coach was making changes to the football practice schedule — it instructed her to download an email attachment to see it. She did. The PDF attachment contained a virus that launched when she opened it, giving crooks access to her computer. Then they had all the sensitive financial information about her employer they needed to steal money.

Among the lessons: make sure the privacy settings on your social media accounts are set so only your friends can see what you post — not the general public.

-

Here's another example. Cybercrooks got a list of company executives and their administrative assistants. Targeting one of those assistants, the crooks sent an urgent text message, appearing to come from an executive, saying an important vendor hadn't paid on time. Money needed to be wired immediately. The text included instructions on where to wire the funds. Of course, the money was wired to the crooks, not to the vendor.

The lesson: if an email, text or phone call is urgent and requires that you take action involving money or entering a password, double check that the message real. If a message makes your blood pressure rise, slow down. You won't get into trouble for taking time to ensure the request is genuine.

-

Example #3; this one caused big trouble at a midsize company. Crooks got hold of a list of stolen employee names and email addresses and sent the entire company an email that appeared to come from IT. The headline said "Revised Vacation Policy." Who isn't interested in that?

By the dozens, employees opened the email and downloaded the attachment, a Word doc. But embedded in the doc was ransomware that locked down the company's computer systems.

The moral of this story: look carefully at the email address an urgent email is coming from. In this case, the senders email address wasn't even close to the company's email address. But employees were so upset over the fake message, they didn't take the time to look.

-

Now, here are examples of spear phishing emails that have been sent to home computers. This first one is common.

An email or text arrives from what appears to be your bank. It arrives at your personal email address and is addressed to you by name. The email address it came from is close to your bank's email address — but not exactly. The email is threatening. It warns that your account is about to be closed because it has been breached and the only way to keep it open is to click on a link in the message and change your password immediately.

The lesson: if you're worried about a message from your bank, call the bank directly. Not the contact information in the email. Instead, look at the back of your bank card, your bank statement or look up their number online.

-

Here's an example of how crooks take time to learn about our personal backgrounds so we'll be more apt to open their spear-phishing emails.

A journalist received an email at his home email address that appeared to come from his college alma mater. The email requested his help judging awards that would be handed out by the college.

Hackers had done their homework. By going to the victim's LinkedIn page, they learned where he'd gone to college. In the email, they were able to mention his professional work history. The crooks were using an email address similar to the college's real email format, so the message seemed to be legitimate.

By simply clicking on a link in the email message, a file would be downloaded, infecting the man's computer. Crooks could then track everything he typed — including all of his passwords and bank account information.

He did click on the link. But it turned out the virus was only dangerous if he was using the Firefox web browser — which is usually very secure. He happened to be using Google Chrome instead. He was just lucky.

The lesson here: before you click on links in emails, look closely at the email address where it came from and make sure the address is exactly what you would expect. Sometimes crooks will replace the letter “O” with a zero or the letter “l” with a one.

Finally, here’s a spear-phishing example that is quite compelling.

Crooks gain access to over your social media account by using a computer program to guess your password. Looking at what you post, they learn the name of your significant other.

They send you an instant message that says “uh-oh, I had a little accident with the car. I took some pictures with my phone. Do you think this is going to be very expensive?”

Clicking on the photo of a fender-bender downloads a virus to your computer.

Of course, your significant other is fine; there was no accident. But your computer is now infected.

Lesson: install anti-virus on your personal computer — doesn’t matter whether you have a Windows or a Mac computer — and set the antivirus software to update itself automatically. And if you get an urgent message from your significant other or other important person in your life, give them a call before clicking on the link in a message.

These spear-phishing emails are becoming more and more common. According to the non-profit cybersecurity organization SANS, practically every large company has been hit. And now, one of every three phishing emails is a spear-phishing email, with a customized message aimed at one person.

I’m Richard Warner.