Banking locally

EVER AFTER

IS KEEPING YOUR INFORMATION SAFE

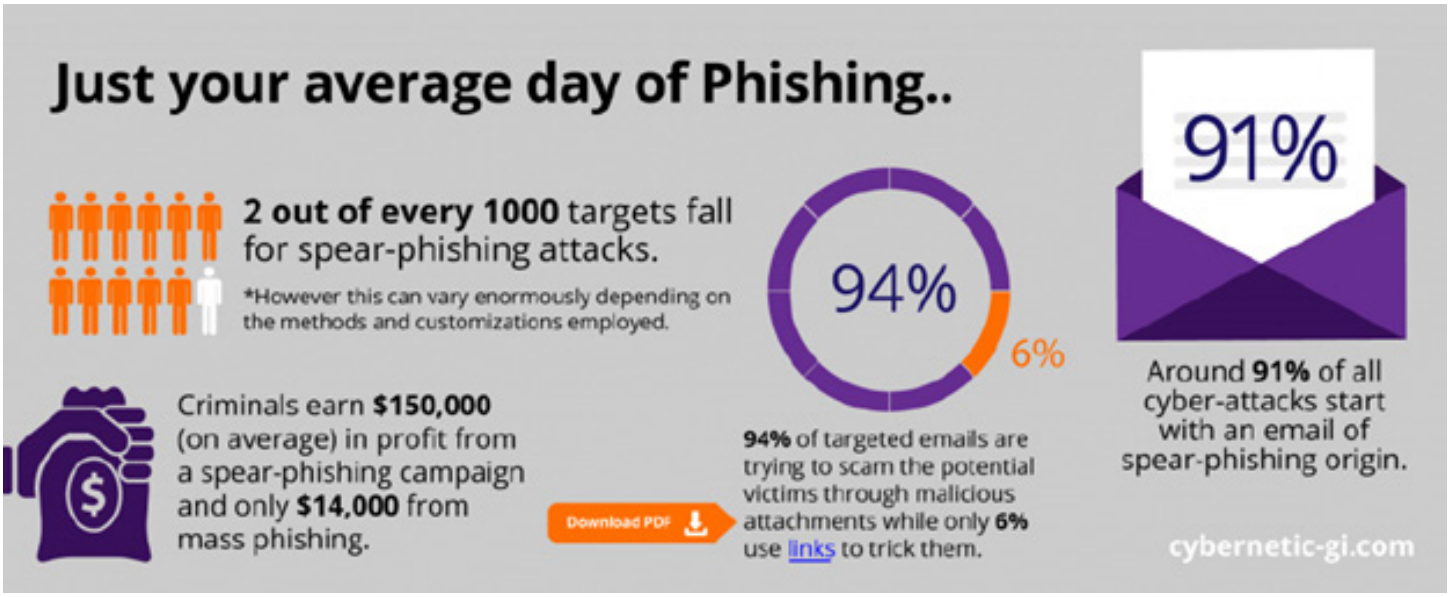
PHISHING TRENDS AND TIPS FOR PROTECTION

In the cyber security world, malware incidents claim many of the headlines. However, phishing scams are actually a bigger threat to consumers and businesses. Phishing email scams have become more widely used because of the way we interact with the world, mostly through mobile devices. Texts, social media posts and messages are meant to be fast ways of communicating, and this leads to prime opportunities for cyber criminals to implement and be successful at phishing. We do not always take a close enough look at emails to check their legitimacy, especially when using a mobile device, and the brief nature of messages in today's digital environment makes it easy to overlook questionable email requests, links or attachments.

Additionally, phishing has become more common because it is easier for attackers to launch phishing attacks quickly. Criminals can shop for and customize phishing toolkits along with everything they need to build an effective scam. And now, the lines between our business and personal lives are blurring on mobile, making our smartphones attractive targets for criminals. Cyber criminals also recognize the heavy reliance on email addresses instead of unique usernames and the frequency in which passwords are reused. In many cases, a high percentage of these stolen credentials provide access to multiple accounts in addition to the account being directly phished. The combination of these realities in today's ever-connected world means that organizations using email addresses as usernames can reasonably assume that a significant portion of their users' credentials have been compromised via phishing attacks at some point or another. There are strategies to use in order to avoid falling victim to phishing scams, protecting personal and financial information in the digital age.

Recent Trends

PhishLabs identified phishing sites residing on more than 170,000 unique domains, a 23% increase over the last year. Attacks targeting government tax authorities have grown more than 300% since 2014. In fact, there were more IRS phishing attacks in January 2016 than there were in all of 2015. The share of attacks against business targets in the United States continues to grow, accounting for more than 81% of all phishing attacks. Of more than 29,000 phish kits analyzed, more than a third used techniques to evade detection. A phish kit is a collection of files containing the files and graphics needed to easily create a phishing site. These are becoming more readily available, making phishing a serious threat to consumers and businesses alike.



Source: Cybernetic Global Intelligence

What Is Phishing and How to Recognize It

Phishing is a cyber-crime in which a target is contacted by email, telephone or text message by someone posing as a legitimate individual or business, intended to lure individuals into providing sensitive data. This data may include personally identifiable information, banking, credit card details and email or account passwords. The information gathered in a phishing scam is then used to fraudulently open new accounts, withdraw funds, make purchases or compromise other accounts on or offline. Recognizing a phishing scam is becoming more complex as cyber criminals get more sophisticated in their efforts. However, here are a few tell-tale signs that you may be the target of phishing:

- **Unusual Sender**
  If you do not recognize the message, sender or even if the message is unexpected, delete it. Hovering your mouse over the sender's email address or clicking on the address on a mobile device allows you to see who originated the message. If it is different from the normal email message received from the company or individual, do not click on attachments or links in the message.

- **Too good to be true**
  These are often "attention seeking" emails designed to get you to click on something. These items could range from anything to winning the lottery, a new phone or a fancy trip. If it sounds too good to be true, do not click on the email or any attachments or links within.

- **Sense of urgency**
  Often phishing scams arrive as time-sensitive communications or offers. Messages may say that you have a short period of time to respond. Don't hesitate to slow it down and do some more investigating.

- **Hyperlinks**
  This is a common tactic for criminals because you can change a character in a hyperlink and redirect an individual to just about any site. Make sure you look at hyperlinks very closely or just delete the email if you do not recognize the sender. Hovering over the hyperlink allows you to see where it is directing you. If it isn't familiar or looks suspicious, do not click.

- **Attachments**
  If you see a file that seems out of place, includes a hyperlink, or has anything other than .txt in the name, do not open it. These files could potentially contain ransomware or a virus to hack your computer or data.

What are tips for avoiding phishing?

In addition to being diligent about the emails you open and the links or attachments you interact with, there are other steps you can take to avoid phishing in the first place. Consider using a spam filter to block message from unknown senders. However, it may be beneficial to review your spam folder every now and again to ensure you aren't missing important, legitimate messages. Also, be diligent about updating settings on your browser, specifically indicating you do not want pop-ups to open without your approval. Finally, be sure to change your passwords on a regular basis, and try not to use the same iteration of passwords on multiple websites or accounts.

What are tips for responding if phishing happens?

- ✓ Change your passwords immediately.
- ✓ Contact the company that was used in the phishing scam so that they may alert others.
- ✓ Scan your computer for malware and v iruses periodically.
- ✓ Watch for identity theft warning signs, like new accounts, new credit inquiries, or other suspicious activity on your credit report.
- ✓ File a report with the Federal Trade Commission after you received a phishing scam email.

With phishing attacks increasing, it's crucial that we raise our awareness and be better positioned to respond when incidents do occur.

Common Questions

- **Is email the only place phishing occurs?**
  No, not necessarily. While email accounts are the easiest to target, phishing attacks may also use instant messaging, social media sites, phone calls and texting to target individuals and gather their personal information. Use the same methods of identifying phishing scams via email with other sources as well.
- **Who is most vulnerable to phishing?**
  Anyone can be a target and ultimately a victim to a phishing attack. However, most individuals who are harmed by phishing are those who are not familiar with technology, such as older adults. Using the tactics above and preventing phishing is especially important to those who may be more vulnerable.

Top Resources

Below are several resources to help you better understand phishing scams. Also, be sure to use My Money Roadmap's Learn Center for more information about cyber security and financial topics relevant in today's ever-connected world.

Protecting Yourself Against Phishing*

What is Phishing*

Federal Trade Commission Cyber Security Tips*

*You will be linking to another website not owned or operated by the bank. We are not responsible for the availability or content of this website and do not represent either the linked website or you, should you enter into a transaction. You are encouraged to review the privacy and security policies which may differ from ours.