

Protect yourself from phishing

Phishing (pronounced: fishing) is an attack that attempts to steal your money, or your identity, by getting you to reveal personal information – such as credit card numbers, bank information, or passwords – on websites that pretend to be legitimate. Cybercriminals typically pretend to be reputable companies, friends, or acquaintances in a fake message, which contains a link to a phishing website.

Phishing is a popular form of cybercrime because of how effective it is. Cybercriminals have been successful using emails, text messages, and direct messages on social media or in video games, to get people to respond with their personal information. The best defense is awareness and knowing what to look for.

Phishing Is Not Just About Emails

Most often, cybercriminals use emails and websites in their phishing attacks. Sometimes they even use both channels in the same scam. For example, they try to get people to click a link in an email, which sends the victims to a phishing site. Phishing calls are also becoming common and increasing rapidly.

Hackers Target Senior because of their lack of knowledge

While phishing attacks were initially targeted at consumers, cybercriminals quickly discovered that businesses are also lucrative targets. In 2018 alone, an estimated 83% of businesses experienced phishing attacks with small and midsize companies being most often targeted. These companies are sought out, as they often do not have the expertise or resources to properly secure their businesses against phishing scams and other types of attacks. Cybercriminals most often target executives, administrative assistants, HR staff and sales team members.

Phishing Sites Can Be Web Pages

Cybercriminals are increasingly using web sites for phishing. Hackers are counting on people being lulled into a false sense of security by the links they send claiming they are safe

Cybercriminals Don't Take Holidays Off

Hackers go phishing 365 days a year and often ramp up their efforts for seasonal events and holidays.

Phishers Are Skilled Impersonators

Cybercriminals often prey on people's compassion, by pretending to be collecting donations for disaster victims or charities. They like to impersonate legitimate contacts and companies to carry out their phishing scams, masquerading as representatives from such popular companies as Microsoft, PayPal, Netflix, UPS and others. When targeting a business, cybercriminals often pretend to be someone within the company, or a client, supplier, or organization that does business with the company.

If you think you've been a victim of a phishing scam, or would like more information; please feel free to contact GRIFFCOMM Helps for assistance.